List of PlugIn IDs

>print

The following plugin IDs have problems associated with them. Select the ID to review more detail.

Plugin id#	# of issues	Plugin name	Severity
32314	2	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	High Severity problem(s) found
57663	1	USN-1339-1 : qemu-kvm vulnerability	High Severity problem(s) found
57616	1	USN-1335-1 : t1lib vulnerabilities	High Severity problem(s) found
57615	1	USN-1334-1 : libxml2 vulnerabilities	High Severity problem(s) found
57449	1	USN-1320-1 : ffmpeg vulnerabilities	High Severity problem(s) found
57436	1	USN-1317-1 : ghostscript vulnerabilities	High Severity problem(s) found
57341	1	USN-1310-1 : libarchive vulnerabilities	High Severity problem(s) found
57315	1	USN-1308-1 : bzip2 vulnerability	High Severity problem(s) found
56970	1	USN-1283-1 : apt vulnerability	High Severity problem(s) found
56870	1	USN-1267-1 : freetype vulnerabilities	High Severity problem(s) found
56860	1	USN-1263-1 :	High Severity

		icedtea-web, openjdk-6, openjdk-6b18 vulnerabilities	problem(s) found
56767	1	USN-1255-1 : libmodplug vulnerabilities	High Severity problem(s) found
57393	1	USN-1254-1 : thunderbird vulnerabilities	High Severity problem(s) found
56775	1	USN-1251-1 : firefox, xulrunner-1.9.2 vulnerabilities	High Severity problem(s) found
56629	1	USN-1237-1 : pam vulnerabilities	High Severity problem(s) found
56580	1	USN-1232-3 : xorg-server vulnerability	High Severity problem(s) found
56563	1	USN-1232-2 : xorg-server regression	High Severity problem(s) found
56555	1	USN-1232-1 : xorg-server vulnerabilities	High Severity problem(s) found
56554	1	USN-1231-1 : php5 vulnerabilities	High Severity problem(s) found
56281	1	USN-1215-1 : apt vulnerabilities	High Severity problem(s) found
56331	1	USN-1213-1 : thunderbird vulnerabilities	High Severity problem(s) found
56330	1	USN-1210-1 : firefox, xulrunner-1.9.2 vulnerabilities	High Severity problem(s) found
56236	1	USN-1209-1 : ffmpeg vulnerabilities	High Severity problem(s) found
56194	1	USN-1206-1 : librsvg vulnerability	High Severity problem(s) found
56140	1	USN-1197-5 : ca-certificates vulnerability	High Severity problem(s) found

56139	1	USN-1197-4 : nss vulnerability	High Severity problem(s) found
56115	1	USN-1197-3 : firefox, xulrunner-1.9.2 vulnerability	High Severity problem(s) found
56089	1	USN-1197-2 : thunderbird vulnerability	High Severity problem(s) found
56036	1	USN-1197-1 : firefox, xulrunner-1.9.2 vulnerability	High Severity problem(s) found
55968	1	USN-1196-1 : ecryptfs-utils vulnerability	High Severity problem(s) found
55967	1	USN-1195-1 : webkit vulnerabilities	High Severity problem(s) found
55858	1	USN-1191-1 : libxfont vulnerability	High Severity problem(s) found
55810	1	USN-1188-1 : ecryptfs-utils vulnerabilities	High Severity problem(s) found
55982	1	USN-1185-1 : thunderbird vulnerabilities	High Severity problem(s) found
55921	1	USN-1184-1 : firefox, xulrunner-1.9.2 vulnerabilities	High Severity problem(s) found
55717	1	USN-1177-1 : qemu-kvm vulnerability	High Severity problem(s) found
55531	1	USN-1165-1 : qemu-kvm vulnerabilities	High Severity problem(s) found
55414	1	USN-1158-1 : curl vulnerabilities	High Severity problem(s) found
55172	1	USN-1154-1 : openjdk-6, openjdk-6b18 vulnerabilities	High Severity problem(s) found

55168	1	USN-1153-1 : libxml2 vulnerability	High Severity problem(s) found
55605	1	USN-1150-1 : thunderbird vulnerabilities	High Severity problem(s) found
55407	1	USN-1149-1 : firefox, xulrunner-1.9.2 vulnerabilities	High Severity problem(s) found
55113	1	USN-1147-1 : gimp vulnerability	High Severity problem(s) found
55108	1	USN-1145-1 : qemu-kvm vulnerabilities	High Severity problem(s) found
55100	1	USN-1138-2 : network-manager, modemmanger update	High Severity problem(s) found
25216	1	Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow	High Severity problem(s) found
42411	1	Microsoft Windows SMB Shares Unprivileged Access	High Severity problem(s) found
55976	1	Apache HTTP Server Byte Range DoS	High Severity problem(s) found
57582	15	SSL Self-Signed Certificate	Medium Severity problem(s) found
51192	15	SSL Certificate signed with an unknown Certificate Authority	Medium Severity problem(s) found
57608	10	SMB Signing Disabled	Medium Severity problem(s) found
26919	8	Microsoft Windows SMB Guest Account Local User Access	Medium Severity problem(s) found
11213	2	HTTP TRACE / TRACK Methods Allowed	Medium Severity problem(s) found
22300	1	Webmin / Usermin Null Byte Filtering	Medium Severity problem(s) found

		Vulnerabilities	
21785	1	Webmin / Usermin miniserv.pl Arbitrary File Disclosure	Medium Severity problem(s) found
11229	1	Web Server info.php / phpinfo.php Detection	Medium Severity problem(s) found
57370	1	USN-1316-1 : t1lib vulnerability	Medium Severity problem(s) found
57357	1	USN-1315-1 : jasper vulnerabilities	Medium Severity problem(s) found
57345	1	USN-1314-1 : python3.1, python3.2 vulnerabilities	Medium Severity problem(s) found
57314	1	USN-1307-1 : php5 vulnerability	Medium Severity problem(s) found
56915	1	USN-1273-1 : pidgin vulnerabilities	Medium Severity problem(s) found
56861	1	USN-1264-1 : bind9 vulnerability	Medium Severity problem(s) found
56778	1	USN-1259-1 : apache2, apache2-mpm-itk vulnerabilities	Medium Severity problem(s) found
56280	1	USN-1214-1 : gimp vulnerability	Medium Severity problem(s) found
56206	1	USN-1207-1 : cups, cupsys vulnerabilities	Medium Severity problem(s) found
56048	1	USN-1199-1 : apache2 vulnerability	Medium Severity problem(s) found
55957	1	USN-1194-1 : foomatic-filters vulnerabilities	Medium Severity problem(s) found
55731	1	USN-1181-1 : libsoup2.4 vulnerability	Medium Severity problem(s) found
55700	1	USN-1176-1 : dbus vulnerability	Medium Severity problem(s) found
55699	1	USN-1175-1 : libpng vulnerabilities	Medium Severity problem(s) found

55689	1	USN-1174-1 : libsndfile vulnerability	Medium Severity problem(s) found
55648	1	USN-1172-1 : logrotate vulnerabilities	Medium Severity problem(s) found
55522	1	USN-1163-1 : bind9 vulnerability	Medium Severity problem(s) found
55114	1	USN-1148-1 : libmodplug vulnerabilities	Medium Severity problem(s) found
55103	1	USN-1140-2 : pam regression	Medium Severity problem(s) found
55102	1	USN-1140-1 : pam vulnerabilities	Medium Severity problem(s) found
55101	1	USN-1139-1 : bind9 vulnerabilities	Medium Severity problem(s) found
55097	1	USN-1136-1 : rdesktop vulnerability	Medium Severity problem(s) found
55095	1	USN-1134-1 : apache2, apr vulnerabilities	Medium Severity problem(s) found
52740	1	USN-1090-1 : linux vulnerabilities	Medium Severity problem(s) found
46803	1	PHP expose_php Information Disclosure	Medium Severity problem(s) found
12218	1	mDNS Detection	Medium Severity problem(s) found
22964	43	Service Detection	Low Severity problem(s) found
11011	20	Microsoft Windows SMB Service Detection	Low Severity problem(s) found
10863	18	SSL Certificate Information	Low Severity problem(s) found
56984	18	SSL / TLS Versions Supported	Low Severity problem(s) found
21643	16	SSL Cipher Suites Supported	Low Severity problem(s) found
19506	13	Nessus Scan Information	Low Severity problem(s) found

35716	13	Ethernet Card Manufacturer Detection	Low Severity problem(s) found
11936	12	OS Identification	Low Severity problem(s) found
10107	12	HTTP Server Type and Version	Low Severity problem(s) found
54615	12	Device Type	Low Severity problem(s) found
45590	12	Common Platform Enumeration (CPE)	Low Severity problem(s) found
10287	11	Traceroute Information	Low Severity problem(s) found
25220	11	TCP/IP Timestamps Supported	Low Severity problem(s) found
10114	11	ICMP Timestamp Request Remote Date Disclosure	Low Severity problem(s) found
24260	11	HyperText Transfer Protocol (HTTP) Information	Low Severity problem(s) found
10150	10	Windows NetBIOS / SMB Remote Host Information Disclosure	Low Severity problem(s) found
10662	10	Web mirroring	Low Severity problem(s) found
10860	10	SMB Use Host SID to Enumerate Local Users	Low Severity problem(s) found
25240	10	Samba Server Detection	Low Severity problem(s) found
10395	10	Microsoft Windows SMB Shares Enumeration	Low Severity problem(s) found
10785	10	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	Low Severity problem(s) found
10859	10	Microsoft Windows SMB	Low Severity problem(s) found

		LsaQueryInformationPolicy Function SID Enumeration	
10394	10	Microsoft Windows SMB Log In Possible	Low Severity problem(s) found
10397	10	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure	Low Severity problem(s) found
17651	10	Microsoft Windows SMB : Obtains the Password Policy	Low Severity problem(s) found
50845	9	OpenSSL Detection	Low Severity problem(s) found
10147	9	Nessus Server Detection	Low Severity problem(s) found
10386	8	Web Server No 404 Error Code Check	Low Severity problem(s) found
20108	8	Web Server / Application favicon.ico Vendor Fingerprinting	Low Severity problem(s) found
20301	8	VMware ESX/GSX Server detection	Low Severity problem(s) found
43815	8	NetBIOS Multiple IP Address Enumeration	Low Severity problem(s) found
24786	8	Nessus Windows Scan Not Performed with Admin Privileges	Low Severity problem(s) found
49704	8	External URLs	Low Severity problem(s) found
11032	3	Web Server Directory Enumeration	Low Severity problem(s) found
10267	3	SSH Server Type and Version Information	Low Severity problem(s) found
10881	3	SSH Protocol Versions Supported	Low Severity problem(s) found
43111	3	HTTP Methods Allowed (per directory)	Low Severity problem(s) found

39521	3	Backported Security Patch Detection (WWW)	Low Severity problem(s) found
39520	3	Backported Security Patch Detection (SSH)	Low Severity problem(s) found
11002	2	DNS Server Detection	Low Severity problem(s) found
40984	2	Browsable Web Directories	Low Severity problem(s) found
18261	2	Apache Banner Linux Distribution Disclosure	Low Severity problem(s) found
10757	1	Webmin Detection	Low Severity problem(s) found
34850	1	Web Server Uses Basic Authentication Without HTTPS	Low Severity problem(s) found
11419	1	Web Server Office File Inventory	Low Severity problem(s) found
56389	1	USN-1226-1 : samba vulnerabilities	Low Severity problem(s) found
55099	1	USN-1138-1 : dbus-glib vulnerability	Low Severity problem(s) found
56468	1	Time of Last System Startup	Low Severity problem(s) found
22869	1	Software Enumeration (SSH)	Low Severity problem(s) found
40665	1	Protected Web Page Detection	Low Severity problem(s) found
26024	1	PostgreSQL Server Detection	Low Severity problem(s) found
10919	1	Open Port Re-check	Low Severity problem(s) found
50686	1	IP Forwarding Enabled	Low Severity problem(s) found
33276	1	Enumerate MAC Addresses via SSH	Low Severity problem(s) found
25202	1	Enumerate IPv6 Interfaces via SSH	Low Severity problem(s) found
25203	1	Enumerate IPv4	Low Severity

		Interfaces via SSH	problem(s) found
35371	1	DNS Server hostname.bind Map Hostname Disclosure	Low Severity problem(s) found
10028	1	DNS Server BIND version Directive Remote Version Disclosure	Low Severity problem(s) found
55472	1	Device Hostname	Low Severity problem(s) found
12634	1	Authenticated Check: OS Name and Installed Package Enumeration	Low Severity problem(s) found
21186	1	AJP Connector Detection	Low Severity problem(s) found

Port (0/tcp)

Plugin ID: 33276
Enumerate MAC Addresses via SSH

Synopsis

This plugin enumerates MAC addresses on a remote host.
List of Hosts

192.168.0.25
Plugin Output

The following MAC addresses exist on the remote host :

- 78:e4:00:f8:53:a7 (interface wlan0)
- 00:50:56:c0:00:08 (interface vmnet8)
- 00:50:56:c0:00:01 (interface vmnet1)
- 20:6a:8a:00:36:f2 (interface eth0)

Description
By connecting to the remote host via SSH with the supplied credentials, this plugin enumerates MAC addresses.

Solution
Disable any unused interfaces.

Risk Factor
None

Plugin publication date: 2008/06/30

Plugin last modification date: 2011/03/21

Port cifs (445/tcp)

Plugin ID: 10395
Microsoft Windows SMB Shares Enumeration

Synopsis

It is possible to enumerate remote network shares.
List of Hosts

192.168.0.67
Plugin Output

Here are the SMB shares available on the remote host when logged as a NULL session:

- print$
- tmp
- opt
- IPC$
- ADMIN$

192.168.0.59
Plugin Output

Here are the SMB shares available on the remote host when logged as tquzmvjt:

- print$
- IPC$

192.168.0.54
Plugin Output

Here are the SMB shares available on the remote host when logged as cbtsmqqf:

- print$
- IPC$

192.168.0.53
Plugin Output

Here are the SMB shares available on the remote host when logged as yfolivrl:

- print$
- IPC$

192.168.0.52
Plugin Output

Here are the SMB shares available on the remote host when logged as xlyewroj:

- print$
- IPC$

192.168.0.41
Plugin Output

Here are the SMB shares available on the remote host when logged as krydcnnq:

- print$
- IPC$

192.168.0.33
Plugin Output

Here are the SMB shares available on the remote host when logged as zqwonzas:

- print$
- IPC$

192.168.0.25
Plugin Output

Here are the SMB shares available on the remote host when logged as uieskptf:

- print$
- IPC$

192.168.0.24
Plugin Output

Here are the SMB shares available on the remote host when logged as yyzdwwxb:

- print$
- IPC$

192.168.0.21
Plugin Output

Here are the SMB shares available on the remote host when logged as a NULL session:

- home
- print$
- IPC$

Description
By connecting to the remote host, Nessus was able to enumerate
the network share names.

Solution
N/A

Risk Factor
None

Plugin publication date: 2000/05/09

Plugin last modification date: 2011/09/14

Port www (8834/tcp)

Plugin ID: 10386
Web Server No 404 Error Code Check

Synopsis

The remote web server does not return 404 error codes.
List of Hosts

192.168.0.59
Plugin Output
The following title tag will be used :
200 Unauthorized

192.168.0.54
Plugin Output
The following title tag will be used :
200 Unauthorized

192.168.0.53
Plugin Output
The following title tag will be used :
200 Unauthorized

192.168.0.52
Plugin Output
The following title tag will be used :
200 Unauthorized

192.168.0.41
Plugin Output
The following title tag will be used :
200 Unauthorized

192.168.0.33
Plugin Output
The following title tag will be used :
200 Unauthorized

192.168.0.25
Plugin Output
The following title tag will be used :
200 Unauthorized

192.168.0.24
Plugin Output
The following title tag will be used :
200 Unauthorized

Description
The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution
n/a

Risk Factor
None

Plugin publication date: 2000/04/28

Plugin last modification date: 2011/10/20

Port www (8834/tcp)

Plugin ID: 56984
SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.
List of Hosts

192.168.0.59
Plugin Output

This port supports SSLv3/TLSv1.0.

192.168.0.54
Plugin Output

This port supports SSLv3/TLSv1.0.

192.168.0.53
Plugin Output

This port supports SSLv3/TLSv1.0.

192.168.0.52
Plugin Output

This port supports SSLv3/TLSv1.0.

192.168.0.41
Plugin Output

This port supports SSLv3/TLSv1.0.

192.168.0.33
Plugin Output

This port supports SSLv3/TLSv1.0.

192.168.0.25
Plugin Output

This port supports SSLv3/TLSv1.0.

192.168.0.24
Plugin Output

This port supports SSLv3/TLSv1.0.

192.168.0.23
Plugin Output

This port supports SSLv3/TLSv1.0.

Description
This script detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution
n/a

Risk Factor
None

Plugin publication date: 2011/12/01

Plugin last modification date: 2012/01/23

Port nessus (1241/tcp)

Plugin ID: 56984
SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.
List of Hosts

192.168.0.59
Plugin Output

This port supports TLSv1.0.

192.168.0.54
Plugin Output

This port supports TLSv1.0.

192.168.0.53

Plugin Output

This port supports TLSv1.0.

192.168.0.52
Plugin Output

This port supports TLSv1.0.

192.168.0.41
Plugin Output

This port supports TLSv1.0.

192.168.0.33
Plugin Output

This port supports TLSv1.0.

192.168.0.25
Plugin Output

This port supports TLSv1.0.

192.168.0.24
Plugin Output

This port supports TLSv1.0.

192.168.0.23
Plugin Output

This port supports TLSv1.0.

Description
This script detects which SSL and TLS versions are supported by the
remote service for encrypting communications.

Solution
n/a

Risk Factor
None

Plugin publication date: 2011/12/01

Plugin last modification date: 2012/01/23

Port (0/tcp)

Plugin ID: 24786
Nessus Windows Scan Not Performed with Admin Privileges

Synopsis

The Nessus scan of this host may be incomplete due to insufficient privileges provided.
List of Hosts

192.168.0.59
Plugin Output
It was not possible to connect to \\BT\ADMIN$

192.168.0.54
Plugin Output
It was not possible to connect to \\BT\ADMIN$

192.168.0.53
Plugin Output
It was not possible to connect to \\BT\ADMIN$

192.168.0.52
Plugin Output
It was not possible to connect to \\BT\ADMIN$

192.168.0.41
Plugin Output
It was not possible to connect to \\BT\ADMIN$

192.168.0.33
Plugin Output
It was not possible to connect to \\BT\ADMIN$

192.168.0.25
Plugin Output
It was not possible to connect to \\BT\ADMIN$

192.168.0.24
Plugin Output
It was not possible to connect to \\BT\ADMIN$

Description
The Nessus scanner testing the remote host has been given SMB credentials to log into the remote host, however these credentials do not have administrative privileges.

Typically, when Nessus performs a patch audit, it logs into the remote host and reads the version of the DLLs on the remote host to determine if a given patch has been applied or not. This is the method Microsoft recommends to determine if a patch has been applied.

If your Nessus scanner does not have administrative privileges when doing a scan, then Nessus has to fall back to perform a patch audit through the registry which may lead to false positives (especially when using third party patch auditing tools) or to false negatives (not all patches can be detected thru the registry).

Solution
Reconfigure your scanner to use credentials with administrative privileges.

Risk Factor
None

Plugin publication date: 2007/03/12

Plugin last modification date: 2011/03/04

Port dns (53/tcp)

Plugin ID: 11002
DNS Server Detection

Synopsis

A DNS server is listening on the remote host.
List of Hosts

192.168.0.67

Description
The remote service is a Domain Name System (DNS) server, which
provides a mapping between hostnames and IP addresses.

Solution
Disable this service if it is not needed or restrict access to
internal hosts only if the service is available externally.

See also
http://en.wikipedia.org/wiki/Domain_Name_System

Risk Factor
None

Plugin publication date: 2003/02/13

Plugin last modification date: 2011/03/11

Port (0/tcp)

Plugin ID: 56194
USN-1206-1 : librsvg vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

List of Hosts

192.168.0.25

Plugin Output

- Installed package : librsvg2-2_2.26.3-0ubuntu1
Fixed package : librsvg2-2_2.26.3-0ubuntu1.1

- Installed package : librsvg2-common_2.26.3-0ubuntu1
Fixed package : librsvg2-common_2.26.3-0ubuntu1.1

Description

Sauli Pahlman discovered that librsvg did not correctly handle
malformed filter names. If a user or automated system were tricked
into processing a specially crafted SVG image, a remote attacker
could gain user privileges.

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1206-1/

Risk Factor

High

CVE

CVE-2011-3146

Other references
USN:1206-1

Patch publication date: 2011/09/13
Plugin publication date: 2011/09/14

Plugin last modification date: 2011/10/21

Port cifs (445/tcp)

Plugin ID: 10785
Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

---

Synopsis

It is possible to obtain information about the remote operating system.
List of Hosts

192.168.0.67
Plugin Output
The remote Operating System is : Unix
The remote native lan manager is : Samba 3.0.20-Debian
The remote SMB Domain Name is : METASPLOITABLE

192.168.0.59
Plugin Output
The remote Operating System is : Unix
The remote native lan manager is : Samba 3.4.7
The remote SMB Domain Name is : BT

192.168.0.54
Plugin Output
The remote Operating System is : Unix
The remote native lan manager is : Samba 3.4.7
The remote SMB Domain Name is : BT

192.168.0.53
Plugin Output
The remote Operating System is : Unix

The remote native lan manager is : Samba 3.4.7
The remote SMB Domain Name is : BT

192.168.0.52
Plugin Output
The remote Operating System is : Unix
The remote native lan manager is : Samba 3.4.7
The remote SMB Domain Name is : BT

192.168.0.41
Plugin Output
The remote Operating System is : Unix
The remote native lan manager is : Samba 3.4.7
The remote SMB Domain Name is : BT

192.168.0.33
Plugin Output
The remote Operating System is : Unix
The remote native lan manager is : Samba 3.4.7
The remote SMB Domain Name is : BT

192.168.0.25
Plugin Output
The remote Operating System is : Unix
The remote native lan manager is : Samba 3.4.7
The remote SMB Domain Name is : BT

192.168.0.24
Plugin Output
The remote Operating System is : Unix
The remote native lan manager is : Samba 3.4.7
The remote SMB Domain Name is : BT

192.168.0.21
Plugin Output
The remote Operating System is : Unix
The remote native lan manager is : Samba 3.0.26a
The remote SMB Domain Name is : UBUNTUVM

Description
It is possible to get the remote operating system name and
version (Windows and/or Samba) by sending an authentication
request to port 139 or 445.

Solution
n/a

Risk Factor
None

Plugin publication date: 2001/10/17

Plugin last modification date: 2011/03/17

Port (0/tcp)

Plugin ID: 55731
USN-1181-1 : libsoup2.4 vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : libsoup2.4-1_2.30.2-0ubuntu0.1
Fixed package : libsoup2.4-1_2.30.2-0ubuntu0.2

Description
It was discovered that libsoup did not properly validate its input
when processing SoupServer requests. A remote attacker could exploit
this to access files via directory traversal.

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1181-1/

Risk Factor
Medium/ CVSS Base Score: 5.0
(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVE
CVE-2011-2524

Other references
USN:1181-1

Patch publication date: 2011/07/28
Plugin publication date: 2011/07/29

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 55858
USN-1191-1 : libxfont vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : libxfont1_1:1.4.1-1
Fixed package : libxfont1_1:1.4.1-1ubuntu0.1

Description

Tomas Hoger discovered that libXfont incorrectly handled certain malformed compressed fonts. An attacker could use a specially crafted font file to cause libXfont to crash, or possibly execute arbitrary code in order to gain privileges.

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1191-1/

Risk Factor

High/ CVSS Base Score: 9.3
(CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVE

CVE-2011-2895

Other references

USN:1191-1

Patch publication date: 2011/08/15
Plugin publication date: 2011/08/16

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 25220
TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

List of Hosts

192.168.0.67

192.168.0.59

192.168.0.54

192.168.0.53

192.168.0.52

192.168.0.41

192.168.0.40

192.168.0.33

192.168.0.24

192.168.0.23

192.168.0.21

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution
n/a

See also
http://www.ietf.org/rfc/rfc1323.txt

Risk Factor
None

Plugin publication date: 2007/05/16

Plugin last modification date: 2011/03/20

Port (0/tcp)

Plugin ID: 55957
USN-1194-1 : foomatic-filters vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : foomatic-filters_4.0.4-0ubuntu1
Fixed package : foomatic-filters_4.0.4-0ubuntu1.1

Description
It was discovered that the foomatic-rip Foomatic filter incorrectly

handled command-line options. An attacker could use this flaw to cause Foomatic to execute arbitrary code as the 'lp' user.

In the default installation, attackers would be isolated by the CUPS AppArmor profile.

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1194-1/

Risk Factor
Medium/ CVSS Base Score: 6.8
(CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVE
CVE-2011-2697
CVE-2011-2964

Other references
USN:1194-1

Patch publication date: 2011/08/22
Plugin publication date: 2011/08/23

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 19506
Nessus Scan Information

Synopsis

Information about the Nessus scan.

List of Hosts

192.168.0.67

Plugin Output

Information about this scan :

Nessus version : 4.4.1
Plugin feed version : 201201250536
Type of plugin feed : HomeFeed (Non-commercial use only)
Scanner IP : 192.168.0.25
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : Detected
Scan Start Date : 2012/1/28 7:01
Scan duration : 339 sec

192.168.0.63

Plugin Output

Information about this scan :

Nessus version : 4.4.1
Plugin feed version : 201201250536
Type of plugin feed : HomeFeed (Non-commercial use only)
Scanner IP : 192.168.0.25
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1

Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Scan Start Date : 2012/1/28 7:01
Scan duration : 376 sec

192.168.0.59
Plugin Output
Information about this scan :

Nessus version : 4.4.1
Plugin feed version : 201201250536
Type of plugin feed : HomeFeed (Non-commercial use only)
Scanner IP : 192.168.0.25
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Scan Start Date : 2012/1/28 7:01
Scan duration : 382 sec

192.168.0.54
Plugin Output
Information about this scan :

Nessus version : 4.4.1
Plugin feed version : 201201250536
Type of plugin feed : HomeFeed (Non-commercial use only)
Scanner IP : 192.168.0.25

Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Scan Start Date : 2012/1/28 7:01
Scan duration : 629 sec

192.168.0.53
Plugin Output
Information about this scan :

Nessus version : 4.4.1
Plugin feed version : 201201250536
Type of plugin feed : HomeFeed (Non-commercial use only)
Scanner IP : 192.168.0.25
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Scan Start Date : 2012/1/28 7:01
Scan duration : 393 sec

192.168.0.52
Plugin Output

Information about this scan :

Nessus version : 4.4.1
Plugin feed version : 201201250536
Type of plugin feed : HomeFeed (Non-commercial use only)
Scanner IP : 192.168.0.25
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Scan Start Date : 2012/1/28 7:01
Scan duration : 378 sec

192.168.0.41
Plugin Output
Information about this scan :

Nessus version : 4.4.1
Plugin feed version : 201201250536
Type of plugin feed : HomeFeed (Non-commercial use only)
Scanner IP : 192.168.0.25
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5

Backports : None
Scan Start Date : 2012/1/28 7:00
Scan duration : 387 sec

192.168.0.40
Plugin Output
Information about this scan :

Nessus version : 4.4.1
Plugin feed version : 201201250536
Type of plugin feed : HomeFeed (Non-commercial use only)
Scanner IP : 192.168.0.25
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : Detected
Scan Start Date : 2012/1/28 7:00
Scan duration : 150 sec

192.168.0.33
Plugin Output
Information about this scan :

Nessus version : 4.4.1
Plugin feed version : 201201250536
Type of plugin feed : HomeFeed (Non-commercial use only)
Scanner IP : 192.168.0.25
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no

Patch management checks : None
CGI scanning : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Scan Start Date : 2012/1/28 7:00
Scan duration : 385 sec

192.168.0.25
Plugin Output
Information about this scan :

Nessus version : 4.4.1
Plugin feed version : 201201250536
Type of plugin feed : HomeFeed (Non-commercial use only)
Scanner IP : 192.168.0.25
Port scanner(s) : netstat
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : yes
Patch management checks : None
CGI scanning : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Scan Start Date : 2012/1/28 7:00
Scan duration : 483 sec

192.168.0.24
Plugin Output
Information about this scan :

Nessus version : 4.4.1
Plugin feed version : 201201250536
Type of plugin feed : HomeFeed (Non-commercial use only)
Scanner IP : 192.168.0.25
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no

Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Scan Start Date : 2012/1/28 7:00
Scan duration : 387 sec

192.168.0.23
Plugin Output
Information about this scan :

Nessus version : 4.4.1
Plugin feed version : 201201250536
Type of plugin feed : HomeFeed (Non-commercial use only)
Scanner IP : 192.168.0.25
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Scan Start Date : 2012/1/28 7:00
Scan duration : 762 sec

192.168.0.21
Plugin Output
Information about this scan :

Nessus version : 4.4.1

Plugin feed version : 201201250536
Type of plugin feed : HomeFeed (Non-commercial use only)
Scanner IP : 192.168.0.25
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : Detected
Scan Start Date : 2012/1/28 7:00
Scan duration : 255 sec

Description

This script displays, for each tested host, information about the
scan itself :

- The version of the plugin set
- The type of plugin feed (HomeFeed or ProfessionalFeed)
- The version of the Nessus Engine
- The port scanner(s) used
- The port range scanned
- Whether credentialed or third-party patch management
checks are possible
- The date of the scan
- The duration of the scan
- The number of hosts scanned in parallel
- The number of checks done in parallel

Solution

n/a

Risk Factor
None

Plugin publication date: 2005/08/26

Plugin last modification date: 2011/12/23

Port (0/tcp)

Plugin ID: 57357
USN-1315-1 : jasper vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : libjasper1_1.900.1-7
Fixed package : libjasper1_1.900.1-7ubuntu0.10.04.1

Description
Jonathan Foote discovered that JasPer incorrectly handled certain malformed JPEG-2000 image files. If a user were tricked into opening a specially crafted JPEG-2000 image file, a remote attacker could cause JasPer to crash or possibly execute arbitrary code with user privileges.

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1315-1/

Risk Factor
Medium/ CVSS Base Score: 6.8
(CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVE
CVE-2011-4516
CVE-2011-4517

Other references
USN:1315-1

Patch publication date: 2011/12/20
Plugin publication date: 2011/12/21

Plugin last modification date: 2011/12/21

Port (0/tcp)

Plugin ID: 56629
USN-1237-1 : pam vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : libpam-modules_1.1.1-2ubuntu5.1

Fixed package : libpam-modules_1.1.1-2ubuntu5.4

Description

Kees Cook discovered that the PAM pam_env module incorrectly handled certain malformed environment files. A local attacker could use this flaw to cause a denial of service, or possibly gain privileges. The default compiler options for affected releases should reduce the vulnerability to a denial of service. (CVE-2011-3148)

Kees Cook discovered that the PAM pam_env module incorrectly handled variable expansion. A local attacker could use this flaw to cause a denial of service. (CVE-2011-3149)

Stephane Chazelas discovered that the PAM pam_motd module incorrectly cleaned the environment during execution of the motd scripts. In certain environments, a local attacker could use this to execute arbitrary code as root, and gain privileges.

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1237-1/

Risk Factor

High

CVE

CVE-2011-3148
CVE-2011-3149
CVE-2011-3628

Other references
USN:1237-1

Patch publication date: 2011/10/24
Plugin publication date: 2011/10/25

Plugin last modification date: 2011/10/25

Port www (8834/tcp)

Plugin ID: 49704
External URLs

Synopsis

Links to external sites were gathered.
List of Hosts

192.168.0.59
Plugin Output

2 external URLs were gathered on this web server :
URL... - Seen on...

http://itunes.apple.com/app/nessus/id390891776?mt=8/ - /
http://www.adobe.com/go/getflash/ - /

192.168.0.54
Plugin Output

2 external URLs were gathered on this web server :
URL... - Seen on...

http://itunes.apple.com/app/nessus/id390891776?mt=8/ - /
http://www.adobe.com/go/getflash/ - /

192.168.0.53
Plugin Output

2 external URLs were gathered on this web server :
URL... - Seen on...

http://itunes.apple.com/app/nessus/id390891776?mt=8/ - /
http://www.adobe.com/go/getflash/ - /

192.168.0.52
Plugin Output

2 external URLs were gathered on this web server :
URL... - Seen on...

http://itunes.apple.com/app/nessus/id390891776?mt=8/ - /
http://www.adobe.com/go/getflash/ - /

192.168.0.41
Plugin Output

2 external URLs were gathered on this web server :
URL... - Seen on...

http://itunes.apple.com/app/nessus/id390891776?mt=8/ - /
http://www.adobe.com/go/getflash/ - /

192.168.0.33
Plugin Output

2 external URLs were gathered on this web server :
URL... - Seen on...

http://itunes.apple.com/app/nessus/id390891776?mt=8/ - /
http://www.adobe.com/go/getflash/ - /

192.168.0.25
Plugin Output

2 external URLs were gathered on this web server :
URL... - Seen on...

http://itunes.apple.com/app/nessus/id390891776?mt=8/ - /
http://www.adobe.com/go/getflash/ - /

192.168.0.24
Plugin Output

2 external URLs were gathered on this web server :
URL... - Seen on...

http://itunes.apple.com/app/nessus/id390891776?mt=8/ - /
http://www.adobe.com/go/getflash/ - /

Description
Nessus gathered HREF links to external sites by crawling the remote
web server.

Solution
n/a

Risk Factor
None

Plugin publication date: 2010/10/04

Plugin last modification date: 2011/08/19

Port www (8834/tcp)

Plugin ID: 24260
HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.
List of Hosts

192.168.0.59
Plugin Output

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Date: Fri, 27 Jan 2012 16:04:08 GMT
Server: NessusWWW
Connection: close
Expires: Fri, 27 Jan 2012 16:04:08 GMT
Content-Length: 6518
Content-Type: text/html
Cache-Control:
Expires: 0
Pragma :

192.168.0.54
Plugin Output

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Date: Fri, 27 Jan 2012 16:09:14 GMT
Server: NessusWWW
Connection: close
Expires: Fri, 27 Jan 2012 16:09:14 GMT
Content-Length: 6518
Content-Type: text/html
Cache-Control:
Expires: 0
Pragma :

192.168.0.53
Plugin Output

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Date: Fri, 27 Jan 2012 23:05:05 GMT

Server: NessusWWW
Connection: close
Expires: Fri, 27 Jan 2012 23:05:05 GMT
Content-Length: 6518
Content-Type: text/html
Cache-Control:
Expires: 0
Pragma :

192.168.0.52
Plugin Output

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Date: Sat, 28 Jan 2012 16:05:35 GMT
Server: NessusWWW
Connection: close
Expires: Sat, 28 Jan 2012 16:05:35 GMT
Content-Length: 6518
Content-Type: text/html
Cache-Control:
Expires: 0
Pragma :

192.168.0.41
Plugin Output

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Date: Fri, 27 Jan 2012 16:04:23 GMT
Server: NessusWWW
Connection: close
Expires: Fri, 27 Jan 2012 16:04:23 GMT
Content-Length: 6518
Content-Type: text/html
Cache-Control:
Expires: 0
Pragma :

192.168.0.33

Plugin Output

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Date: Fri, 27 Jan 2012 16:04:07 GMT
Server: NessusWWW
Connection: close
Expires: Fri, 27 Jan 2012 16:04:07 GMT
Content-Length: 6518
Content-Type: text/html
Cache-Control:
Expires: 0
Pragma :

192.168.0.25
Plugin Output

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Date: Fri, 27 Jan 2012 23:03:46 GMT
Server: NessusWWW
Connection: close
Expires: Fri, 27 Jan 2012 23:03:46 GMT
Content-Length: 6518
Content-Type: text/html
Cache-Control:
Expires: 0
Pragma :

192.168.0.24
Plugin Output

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Date: Fri, 27 Jan 2012 16:03:58 GMT
Server: NessusWWW

Connection: close
Expires: Fri, 27 Jan 2012 16:03:58 GMT
Content-Length: 6518
Content-Type: text/html
Cache-Control:
Expires: 0
Pragma :

Description
This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution
n/a

Risk Factor
None

Plugin publication date: 2007/01/30

Plugin last modification date: 2011/05/31

Port (80/tcp)

Plugin ID: 24260
HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

List of Hosts

192.168.0.67
Plugin Output

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

Date: Fri, 27 Jan 2012 23:08:05 GMT
Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
Last-Modified: Wed, 17 Mar 2010 14:08:25 GMT
ETag: "107f7-2d-481ffa5ca8840"
Accept-Ranges: bytes
Content-Length: 45
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

192.168.0.40
Plugin Output

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

Date: Fri, 27 Jan 2012 16:04:11 GMT
Server: Apache/2.2.16 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 2608
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=UTF-8

192.168.0.21
Plugin Output

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : GET,HEAD,POST,OPTIONS,TRACE
Headers :

Date: Fri, 27 Jan 2012 22:51:48 GMT

Server: Apache/2.2.4 (Ubuntu) PHP/5.2.3-1ubuntu6
X-Powered-By: PHP/5.2.3-1ubuntu6
Content-Length: 295
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html

Description
This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution
n/a

Risk Factor
None

Plugin publication date: 2007/01/30

Plugin last modification date: 2011/05/31

Port (0/tcp)

Plugin ID: 55414
USN-1158-1 : curl vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : libcurl3_7.19.7-1ubuntu1
Fixed package : libcurl3_7.19.7-1ubuntu1.1

- Installed package : libcurl3-gnutls_7.19.7-1ubuntu1
Fixed package : libcurl3-gnutls_7.19.7-1ubuntu1.1

Description
Richard Silverman discovered that when doing GSSAPI authentication, libcurl unconditionally performs credential delegation, handing the server a copy of the client's security credential. (CVE-2011-2192)

Wesley Miaw discovered that when zlib is enabled, libcurl does not properly restrict the amount of callback data sent to an application that requests automatic decompression. This might allow an attacker to cause a denial of service via an application crash or possibly execute arbitrary code with the privilege of the application. This issue only affected Ubuntu 8.04 LTS and Ubuntu 10.04 LTS. (CVE-2010-0734)

USN 818-1 fixed an issue with curl's handling of SSL certificates with zero bytes in the Common Name. Due to a packaging error, the fix for this issue was not being applied during the build. This issue only affected Ubuntu 8.04 LTS. We apologize for the error. (CVE-2009-2417)

Original advisory details:

Scott Cantor discovered that curl did not correctly handle SSL certificates with zero bytes in the Common Name. A remote attacker could exploit this to perform a man in the middle attack to view sensitive information or alter encrypted communications.

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1158-1/

Risk Factor
High/ CVSS Base Score: 7.5
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVE
CVE-2009-2417
CVE-2010-0734
CVE-2011-2192

Other references
USN:1158-1
CWE:310

Patch publication date: 2011/06/24
Plugin publication date: 2011/06/24

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 10919
Open Port Re-check

Synopsis

Previously open ports are now closed.
List of Hosts

192.168.0.23
Plugin Output

Port 8834 was detected as being open but is now closed
Port 1241 was detected as being open but is now closed

Description

One of several ports that were previously open are now closed or unresponsive.

There are numerous possible causes for this failure :
- The scan may have caused a service to freeze or stop running.
- An administrator may have stopped a particular service during the scanning process.

This might be an availability problem related to the following reasons :
- A network outage has been experienced during the scan, and the remote network cannot be reached from the Vulnerability Scanner any more.
- This Vulnerability Scanner has been blacklisted by the system administrator or by automatic intrusion detection/prevention systems which have detected the vulnerability assessment.
- The remote host is now down, either because a user turned it off during the scan or because a select denial of service was effective.

In any case, the audit of the remote host might be incomplete and may need to be done again

---

Solution

- increase checks_read_timeout and/or reduce max_checks
- disable your IPS during the Nessus scan

Risk Factor

None

Plugin publication date: 2002/03/19

Plugin last modification date: 2011/03/07

Port (0/tcp)

Plugin ID: 55168
USN-1153-1 : libxml2 vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : libxml2_2.7.6.dfsg-1ubuntu1.1
Fixed package : libxml2_2.7.6.dfsg-1ubuntu1.2

Description
Chris Evans discovered that libxml2 incorrectly handled memory allocation. If an application using libxml2 opened a specially crafted XML file, an attacker could cause a denial of service or possibly execute code as the user invoking the program.

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1153-1/

Risk Factor
High/ CVSS Base Score: 9.3
(CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVE
CVE-2011-1944

Other references
USN:1153-1

Patch publication date: 2011/06/16
Plugin publication date: 2011/06/17

Plugin last modification date: 2011/10/21

Port (0/icmp)

Plugin ID: 10114
ICMP Timestamp Request Remote Date Disclosure

Synopsis

It is possible to determine the exact time set on the remote host.
List of Hosts

192.168.0.67
Plugin Output
The difference between the local and remote clocks is -107 seconds.

192.168.0.59
Plugin Output
The difference between the local and remote clocks is 25150 seconds.

192.168.0.54
Plugin Output
The difference between the local and remote clocks is 25095 seconds.

192.168.0.53
Plugin Output
The difference between the local and remote clocks is -107 seconds.

192.168.0.52

Plugin Output
The difference between the local and remote clocks is 25039 seconds.

192.168.0.41
Plugin Output
The difference between the local and remote clocks is 25096 seconds.

192.168.0.40
Plugin Output
The difference between the local and remote clocks is 25094 seconds.

192.168.0.33
Plugin Output
The difference between the local and remote clocks is 25093 seconds.

192.168.0.24
Plugin Output
The difference between the local and remote clocks is 25095 seconds.

192.168.0.23
Plugin Output
The difference between the local and remote clocks is 25095 seconds.

192.168.0.21
Plugin Output
The difference between the local and remote clocks is 698 seconds.

Description
The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine.

This may help an attacker to defeat all time-based authentication protocols.

Solution
Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk Factor
None

CVE
CVE-1999-0524

Other references
OSVDB:94
CWE:200

Vulnerability publication date: 1995/01/01
Plugin publication date: 1999/08/01

Plugin last modification date: 2011/11/15

Port (10000/tcp)

Plugin ID: 10107
HTTP Server Type and Version

Synopsis

A web server is running on the remote host.
List of Hosts

192.168.0.21
Plugin Output
The remote web server type is :

MiniServ/0.01

Description
This plugin attempts to determine the type and the version of the
remote web server.

Solution
n/a

Risk Factor
None

Plugin publication date: 2000/01/04

Plugin last modification date: 2011/11/30

Port www (8834/tcp)

Plugin ID: 10107
HTTP Server Type and Version

Synopsis

A web server is running on the remote host.
List of Hosts

192.168.0.59
Plugin Output
The remote web server type is :

NessusWWW

192.168.0.54
Plugin Output
The remote web server type is :

NessusWWW

192.168.0.53
Plugin Output
The remote web server type is :

NessusWWW

192.168.0.52
Plugin Output
The remote web server type is :

NessusWWW

192.168.0.41
Plugin Output
The remote web server type is :

NessusWWW

192.168.0.33
Plugin Output
The remote web server type is :

NessusWWW

192.168.0.25
Plugin Output
The remote web server type is :

NessusWWW

192.168.0.24
Plugin Output
The remote web server type is :

NessusWWW

Description
This plugin attempts to determine the type and the version of the
remote web server.

Solution
n/a

Risk Factor

None

Plugin publication date: 2000/01/04

Plugin last modification date: 2011/11/30

Port (80/tcp)

Plugin ID: 10107
HTTP Server Type and Version

Synopsis

A web server is running on the remote host.
List of Hosts

192.168.0.67
Plugin Output
The remote web server type is :

Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch

You can set the directive 'ServerTokens Prod' to limit the information
emanating from the server in its response headers.

192.168.0.40
Plugin Output
The remote web server type is :

Apache/2.2.16 (Ubuntu)

You can set the directive 'ServerTokens Prod' to limit the information
emanating from the server in its response headers.

192.168.0.21
Plugin Output
The remote web server type is :

Apache/2.2.4 (Ubuntu) PHP/5.2.3-1ubuntu6

You can set the directive 'ServerTokens Prod' to limit the information
emanating from the server in its response headers.

Description
This plugin attempts to determine the type and the version of the
remote web server.

Solution
n/a

Risk Factor
None

Plugin publication date: 2000/01/04

Plugin last modification date: 2011/11/30

Port (0/tcp)

Plugin ID: 55522
USN-1163-1 : bind9 vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : libdns64_1:9.7.0.dfsg.P1-1ubuntu0.1
Fixed package : libdns64_1:9.7.0.dfsg.P1-1ubuntu0.3

Description

It was discovered that Bind incorrectly handled certain specially crafted packets. A remote attacker could use this flaw to cause Bind to stop responding, resulting in a denial of service.

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1163-1/

Risk Factor
Medium/ CVSS Base Score: 5.0
(CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVE
CVE-2011-2464

Other references
USN:1163-1

Patch publication date: 2011/07/05
Plugin publication date: 2011/07/06

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 56139
USN-1197-4 : nss vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : libnss3-1d_3.12.9+ckbi-1.82-0ubuntu0.10.04.1
Fixed package : libnss3-1d_3.12.9+ckbi-1.82-0ubuntu0.10.04.3

Description
USN-1197-1 and USN-1197-3 addressed an issue in Firefox and Xulrunner pertaining to the Dutch Certificate Authority DigiNotar mis-issuing fraudulent certificates. This update provides the corresponding update for the Network Security Service libraries (NSS).

Original advisory details: USN-1197-1

It was discovered that Dutch Certificate Authority DigiNotar, had mis-issued multiple fraudulent certificates. These certificates could allow an attacker to perform a 'man in the middle' (MITM) attack which would make the user believe their connection is secure, but is actually being monitored.

For the protection of its users, Mozilla has removed the DigiNotar certificate. Sites using certificates issued by DigiNotar will need to seek another certificate vendor.

We are currently aware of a regression that blocks one of two Staat der Nederlanden root certificates which are believed to still be secure. This regression is being tracked at https://launchpad.net/bugs/838322.

USN-1197-3

USN-1197-1 partially addressed an issue with Dutch Certificate Authority DigiNotar mis-issuing fraudulent certificates. This update actively distrusts the DigiNotar root certificate as well as several intermediary certificates. Also included in this list of distrusted certificates are the 'PKIOverheid' (PKIGovernment) intermediates under DigiNotar's control that did not chain to DigiNotar's root and were not previously blocked.

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1197-4/

Risk Factor
High

Other references
USN:1197-4

Patch publication date: 2011/09/08
Plugin publication date: 2011/09/09

Plugin last modification date: 2011/10/21

Port cifs (445/tcp)

Plugin ID: 57608
SMB Signing Disabled

Synopsis

Signing is disabled on the remote SMB server.
List of Hosts

192.168.0.67

192.168.0.59

192.168.0.54

192.168.0.53

192.168.0.52

192.168.0.41

192.168.0.33

192.168.0.25

192.168.0.24

192.168.0.21

Description
Signing is disabled on the remote SMB server. This can allow man-in-the-middle attacks against the SMB server.

Solution
Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

See also
http://support.microsoft.com/kb/887429
http://technet.microsoft.com/en-us/library/cc786681%28WS.10%29.aspx
http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html

---

Risk Factor
Medium/ CVSS Base Score: 5.0
(CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N)

Vulnerability publication date: 2012/01/17
Plugin publication date: 2012/01/19

Plugin last modification date: 2012/01/19

Port (0/tcp)

Plugin ID: 55968
USN-1196-1 : ecryptfs-utils vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : ecryptfs-utils_83-0ubuntu3.1
Fixed package : ecryptfs-utils_83-0ubuntu3.2.10.04.2

Description
It was discovered that eCryptfs incorrectly handled permissions when modifying the mtab file. A local attacker could use this flaw to manipulate the mtab file, and possibly unmount arbitrary locations, leading to a denial of service.

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1196-1/

Risk Factor

High

CVE
CVE-2011-3145

Other references
USN:1196-1

Patch publication date: 2011/08/23
Plugin publication date: 2011/08/24

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 55810
USN-1188-1 : ecryptfs-utils vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : ecryptfs-utils_83-0ubuntu3.1
Fixed package : ecryptfs-utils_83-0ubuntu3.2.10.04.1

Description
Vasiliy Kulikov and Dan Rosenberg discovered that eCryptfs incorrectly validated permissions on the requested mountpoint. A local attacker could use this flaw to mount to arbitrary locations, leading to privilege escalation. (CVE-2011-1831)

Vasiliy Kulikov and Dan Rosenberg discovered that eCryptfs incorrectly validated permissions on the requested mountpoint. A local attacker could use this flaw to unmount to arbitrary locations, leading to a denial of service. (CVE-2011-1832)

Vasiliy Kulikov and Dan Rosenberg discovered that eCryptfs incorrectly validated permissions on the requested source directory. A local attacker could use this flaw to mount an arbitrary directory, possibly leading to information disclosure. A pending kernel update will provide the other half of the fix for this issue. (CVE-2011-1833)

Dan Rosenberg and Marc Deslauriers discovered that eCryptfs incorrectly handled modifications to the mtab file when an error occurs. A local attacker could use this flaw to corrupt the mtab file, and possibly unmount arbitrary locations, leading to a denial of service. (CVE-2011-1834)

Marc Deslauriers discovered that eCryptfs incorrectly handled keys when setting up an encrypted private directory. A local attacker could use this flaw to manipulate keys during creation of a new user. (CVE-2011-1835)

Marc Deslauriers discovered that eCryptfs incorrectly handled permissions during recovery. A local attacker could use this flaw to possibly access another user's data during the recovery process. This issue only applied to Ubuntu 11.04. (CVE-2011-1836)

Vasiliy Kulikov discovered that eCryptfs incorrectly handled lock counters. A local attacker could use this flaw to possibly overwrite arbitrary files. The default symlink restrictions in Ubuntu 10.10 and 11.04 should protect against this issue. (CVE-2011-1837)

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1188-1/

Risk Factor
High

CVE
CVE-2011-1831
CVE-2011-1832
CVE-2011-1833
CVE-2011-1834
CVE-2011-1835
CVE-2011-1836
CVE-2011-1837

Other references
USN:1188-1

Patch publication date: 2011/08/09
Plugin publication date: 2011/08/10

Plugin last modification date: 2011/10/21

Port cifs (445/tcp)

Plugin ID: 42411
Microsoft Windows SMB Shares Unprivileged Access

Synopsis

It is possible to access a network share.
List of Hosts

192.168.0.67
Plugin Output

The following shares can be accessed using a NULL session :

- tmp - (readable,writable)
+ Content of this share :
..
.ICE-unix

.X11-unix
4556.jsvc_up

Description

The remote has one or more Windows shares that can be accessed through the network with the given credentials.

Depending on the share rights, it may allow an attacker to read/write confidential data.

Solution

To restrict access under Windows, open Explorer, do a right click on each share, go to the 'sharing' tab, and click on 'permissions'.

Risk Factor

High/ CVSS Base Score: 7.5
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)
CVSS Temporal Score: 7.5(CVSS2#E:H/RL:U/RC:ND)

CVE

CVE-1999-0519
CVE-1999-0520

Bugtraq ID

8026

Other references

OSVDB:299

Vulnerability publication date: 1999/07/14
Plugin publication date: 2009/11/06

Plugin last modification date: 2011/03/27

Ease of exploitability: No exploit is required

Port (0/tcp)

Plugin ID: 56580
USN-1232-3 : xorg-server vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : xserver-xorg-core_2:1.7.6-2ubuntu7.6
Fixed package : xserver-xorg-core_2:1.7.6-2ubuntu7.10

Description
USN-1232-1 fixed vulnerabilities in the X.Org X server. A regression was found on Ubuntu 10.04 LTS that affected GLX support, and USN-1232-2 was released to temporarily disable the problematic security fix. This update includes a revised fix for CVE-2010-4818.

We apologize for the inconvenience.

Original advisory details:

It was discovered that the X server incorrectly handled certain malformed input. An authorized attacker could exploit this to cause the X server to crash, leading to a denial or service, or possibly execute arbitrary code with root privileges. This issue only affected Ubuntu 10.04 LTS and 10.10. (CVE-2010-4818)

It was discovered that the X server incorrectly handled certain malformed input. An authorized attacker could exploit this to cause the X server to crash, leading to a denial or service, or possibly

read arbitrary data from the X server process. This issue only affected Ubuntu 10.04 LTS. (CVE-2010-4819)

Vladz discovered that the X server incorrectly handled lock files. A local attacker could use this flaw to determine if a file existed or not. (CVE-2011-4028)

Vladz discovered that the X server incorrectly handled setting lock file permissions. A local attacker could use this flaw to gain read permissions on arbitrary files and view sensitive information. (CVE-2011-4029)

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1232-3/

Risk Factor
High

CVE
CVE-2010-4818
CVE-2010-4819
CVE-2011-4028
CVE-2011-4029

Other references
USN:1232-3

Patch publication date: 2011/10/20
Plugin publication date: 2011/10/21

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 22869
Software Enumeration (SSH)

Synopsis

It is possible to enumerate installed software on the remote host, via SSH.
List of Hosts

192.168.0.25
Plugin Output

Here is the list of packages installed on the remote Linux system :

```
+++-====================================-========================================
===========-============================================================================
=============================================================================================
==========
Desired=Unknown/Install/Remove/Purge/Hold
iU virtualbox-4.1 4.1.8-75467~Ubuntu~maverick Oracle VM VirtualBox
ii 0trace 1.0-bt4 0trace is a traceroute tool that can be run within an existing, open TCP
connection - therefore bypassing some types of stateful packet filters with ease.
ii 3proxy 0.6.1-bt2 3APA3A 3proxy tiny proxy server
ii ace 1.10-bt2 ACE (Automated Corporate Enumerator) is a simple yet powerful VoIP
Corporate Directory enumeration tool that mimics the behavior of an IP Phone in order t
ii acetoneiso 2.2.1-1 feature-rich application to mount and manage CD/DVD images
ii adduser 3.112ubuntu1 add and remove users and groups
ii admsnmp 0.1-bt3 SNMP audit scanner.
ii adobereader-enu 9.4.6 Adobe Reader allows you to view navigate and print PDF files.
This version adds advanced forms support (save), better integration with Adobe Acrobat
workf
ii afflib 3.6.10-bt1 An open source implementation of AFF written in C.
ii air 2.0.0-bt2 AIR is a GUI front-end to dd/dc3dd designed for easily creating forensic
images.
ii aircrack-ng 1.1-bt9 Aircrack-ng wireless exploitation and enumeration suite
ii akonadi-server 1.4.0-0ubuntu1~lucid1~ppa3 Akonadi PIM storage service
ii alsa-base 1.0.22.1+dfsg-0ubuntu3 ALSA driver configuration files
ii alsa-tools 1.0.22-0ubuntu1 Console based ALSA utilities for specific hardware
ii alsa-utils 1.0.22-0ubuntu5 ALSA utilities
ii amap 5.2-bt4 Amap is a next-generation tool for assistingnetwork penetration testing. It
```

performs fast and reliable application protocol detection, independant on the
ii and 1.2.2-4 Auto Nice Daemon
ii ant 1.7.1-4ubuntu1.1 Java based build tool like make
ii ant-gcj 1.7.1-4ubuntu1.1 Java based build tool like make
ii ant-optional 1.7.1-4ubuntu1.1 Java based build tool like make - optional libraries
ii ant-optional-gcj 1.7.1-4ubuntu1.1 Java based build tool like make - API documentation and manual
ii anthy 9100h-0ubuntu2 input method for Japanese - backend, dictionary and utility
ii apache2 2.2.14-5ubuntu8.4 Apache HTTP Server metapackage
ii apache2-mpm-prefork 2.2.14-5ubuntu8.4 Apache HTTP Server - traditional non-threaded model
ii apache2-utils 2.2.14-5ubuntu8.4 utility programs for webservers
ii apache2.2-bin 2.2.14-5ubuntu8.4 Apache HTTP Server common binary files
ii apache2.2-common 2.2.14-5ubuntu8.4 Apache HTTP Server common files
ii app-install-data 0.10.04.7 Ubuntu applications (data files)
ii apport 1.13.3-0ubuntu2 automatically generate crash reports for debugging
ii apport-symptoms 0.9 symptom scripts for apport
ii apt 0.7.25.3ubuntu9.4 Advanced front-end for dpkg
ii apt-transport-https 0.7.25.3ubuntu9.4 APT https transport
ii apt-utils 0.7.25.3ubuntu9.4 APT utility programs
ii apt-xapian-index 0.25ubuntu2 maintenance tools for a Xapian index of Debian packages
ii aptitude 0.4.11.11-1ubuntu10 terminal-based package manager
ii archey 0.2.8 Archey
ii aria2 1.8.0-1 High speed download utility
ii ark 4:4.5.3-0ubuntu1~lucid1~ppa1 archive utility for KDE 4
ii arp-scan 1.6-2 arp scanning and fingerprinting tool
ii arptables 0.0.3.3-3 ARP table administration
ii asleap 2.2-bt1 Demonstrates a serious deficiency in proprietary Cisco LEAP networks.
ii asp-auditor 2.2-bt2 Look for common misconfigurations and information leaks in ASP.NET applications.
ii aspell 0.60.6-3ubuntu1 GNU Aspell spell-checker
ii aspell-en 6.0-0-5.1ubuntu3 English dictionary for GNU Aspell
ii at 3.1.11-1ubuntu5.1 Delayed job execution and batch processing
ii audacious 2.3-1ubuntu4 small and fast audio player which supports lots of formats
ii audacious-plugins 2.3-1ubuntu4 Base plugins for audacious
ii audacity 1.3.12-2 A fast, cross-platform audio editor
ii audacity-data 1.3.12-2 A fast, cross-platform audio editor (data)
ii autoconf 2.65-3ubuntu1 automatic configure script builder
ii automake 1:1.11.1-1 A tool for generating GNU Standards-compliant Makefiles
ii autopsy 2.24-bt0 A graphical interface to TSK.
ii autoscan 1.50-bt0 A network scanner (discovering and managing application).
ii autotools-dev 20090611.1 Update infrastructure for config.{guess,sub} files
ii avahi-daemon 0.6.25-1ubuntu6.2 Avahi mDNS/DNS-SD daemon
ii avast4workstation 1.3.0 avast! antivirus for Linux
ii avidemux 1:2.5.2-0ubuntu3 a free video editor - GTK version
ii avidemux-common 1:2.5.2-0ubuntu3 a free video editor - Internationalization files
ii avidemux-plugins-common 1:2.5.2-0ubuntu3 a free video editor - common files for plugins

ii avidemux-plugins-gtk 1:2.5.2-0ubuntu3 a free video editor - GTK plugins
ii axel 2.4-1 light download accelerator - console version
ii backtrack-bash-profile 1.0-bt2 bash profile and bashrc files
ii backtrack-bootsplash 1.0-bt2 BackTrack bootsplash
ii backtrack-kde4-essential 1.5-bt3 KDE4 Essential Environment for BackTrack 5
ii backtrack-menu-icons 1.5-bt3 BackTrack Menu Icons
ii backtrack-utils 1.3-bt3 Small bash scripts and utilities, as well as core apps that need to be in the build.
ii backtrack-wallpapers 1.1-bt0 BackTrack Wallpapers
ii base-files 5.0.0ubuntu20.10.04.3 Debian base system miscellaneous files
ii base-passwd 3.5.22 Debian base system master password and group files
ii bash 4.1-2ubuntu3 The GNU Bourne Again SHell
ii bash-completion 1:1.1-3ubuntu2 programmable completion for the bash shell
ii bc 1.06.95-2 The GNU bc arbitrary precision calculator language
ii bchunk 1.2.0-11 CD image format conversion from bin/cue to iso/cdr
ii bed 0.5-bt1 BED is a program which is designed to check daemons for potential buffer overflows, format strings et. al.
ii beef 0.4.0.0-bt2 BeEF, the Browser Exploitation Framework is a professional security tool provided for lawful research and testing purposes. It allows the experienced pene
ii beef-ng 0.4.2.8-bt1 The Browser Exploitation Framework (BeEF) is a powerful professional security tool. BeEF is pioneering techniques that provide the experienced penetration
ii bind9-host 1:9.7.0.dfsg.P1-1ubuntu0.1 Version of 'host' bundled with BIND 9.X
ii binfmt-support 1.2.18 Support for extra binary formats
ii binutils 2.20.1-3ubuntu7.1 The GNU assembler, linker and binary utilities
ii bison 1:2.4.1.dfsg-3 A parser generator that is compatible with YACC
ii bkhive 1.1.1-1 Dump the syskey bootkey from a Windows NT/2K/XP system hive
ii bleachbit 0.7.3-1 delete unnecessary files from the system
ii blindelephant 1.0-bt3 Blind Elephant is an open-source generic web application fingerprinter that produces results by examining a small set of static files.
ii blt 2.4z-4.2 the BLT extension library for Tcl/Tk - run-time package
ii bluediving 0.9-bt1 Bluediving is a Bluetooth penetration testing suite.
ii bluefish 1.0.7-6ubuntu2 advanced Gtk+ HTML editor
ii bluemaho 090417-bt0 BlueMaho is GUI-shell (interface) for suite of tools for testing security of bluetooth devices. It is freeware, opensource, written on python, uses wxPyho
ii bluetooth 4.60-0ubuntu8 Bluetooth support
ii bluez 4.91-bt0 BlueZ is official Linux Bluetooth protocol stack. It is an Open Source project distributed under GNU General Public License (GPL). BlueZ kernel is part of
ii bluez-alsa 4.60-0ubuntu8 Bluetooth audio support
ii bluez-cups 4.60-0ubuntu8 Bluetooth printer driver for CUPS
ii bluez-gstreamer 4.60-0ubuntu8 Bluetooth GStreamer support
ii bluez-hcidump 1.42-1build1 Analyses Bluetooth HCI packets
ii bluez-utils 4.60-0ubuntu8 Transitional package
ii bmon 2.0.1-3 portable bandwidth monitor and rate estimator
ii bogl-bterm 0.1.18-3ubuntu4 Ben's Own Graphics Library - graphical terminal
ii braa 0.82-bt2 Braa is a tool for making SNMP queries.
ii brasero 2.30.2-0ubuntu1.1 CD/DVD burning application for GNOME
ii brasero-common 2.30.2-0ubuntu1.1 Common files for the Brasero CD burning application

and library
ii bridge-utils 1.4-5ubuntu2 Utilities for configuring the Linux Ethernet bridge
ii bsdmainutils 8.0.1ubuntu1 collection of more utilities from FreeBSD
ii bsdutils 1:2.17.2-0ubuntu1.10.04.2 Basic utilities from 4.4BSD-Lite
ii bt-system-menu-icons 1.0-bt1 BackTrack system menu icons
ii btscanner 2.1-bt0 btscanner is a tool designed specifically to extract as much information as possible from a Bluetooth device without the requirement to pair. A detailed i
ii build-essential 11.4build1 Informational list of build-essential packages
ii bulk-extractor 0.7.18-bt0 A C++ program that scans a disk image (or any other file) and extracts useful information.
ii burpsuite 1.4.01-bt0 integrated platform for performing security testing of web applications
ii busybox-initramfs 1:1.13.3-1ubuntu11 Standalone shell setup for initramfs
ii busybox-static 1:1.13.3-1ubuntu11 Standalone rescue shell with tons of builtin utilities
ii byobu 2.68-0ubuntu1.1 a set of useful profiles and a profile-switcher for GNU screen
ii bzip2 1.0.5-4ubuntu0.1 high-quality block-sorting file compressor - utilities
ii ca-certificates 20090814 Common CA certificates
ii ca-certificates-java 20100406ubuntu1 Common CA certificates (JKS keystore)
ii cabextract 1.2-3+lenny1build0.10.04.1 a program to extract Microsoft Cabinet files
ii cadaver 0.23.3-1 command-line WebDAV client
ii cairo-dock 2.4.0~2-1ubuntu0~lucid A light and eye-candy dock to launch your programs (metapackage)
ii cairo-dock-core 2.4.0~2-1ubuntu0~lucid A light and eye-candy dock to launch your programs (core package)
ii cairo-dock-data 2.4.0~2-1ubuntu0~lucid A light and eye-candy dock to launch your programs (common files)
ii cairo-dock-plug-ins 2.4.0~2.1-1ubuntu0~lucid A set of plug-ins for cairo-dock
ii cairo-dock-plug-ins-data 2.4.0~2.1-1ubuntu0~lucid Common files for cairo-dock-plug-ins
ii cairo-dock-plug-ins-integration 2.4.0~2.1-1ubuntu0~lucid Two plug-ins for cairo-dock for a better integration in GNOME or Xfce
ii casper 1.236.2 Run a "live" preinstalled system from read-only media
ii cdparanoia 3.10.2+debian-9 audio extraction tool for sampling CDs
ii cdrdao 1:1.2.2-18ubuntu4 records CDs in Disk-At-Once (DAO) mode
ii cewl 4.1-bt1 CeWL, the Custom Word List generator.
ii checkinstall 1.6.1-10 installation tracker
ii chkconfig 11.0-79.1-2 system tool to enable or disable system services
ii chkrootkit 0.49-3 rootkit detector
ii chm2pdf 0.9.1-1.1ubuntu3 A Python script that converts CHM files into PDF files
ii chntpw 100627-bt0 The Offline NT Password Editor
ii chromium-browser 11.0.696.65~r84435-0ubuntu0.10.04.1 Chromium browser
ii chromium-browser-inspector 11.0.696.65~r84435-0ubuntu0.10.04.1 page inspector for the chromium-browser
ii chromium-browser-l10n 11.0.696.65~r84435-0ubuntu0.10.04.1 chromium-browser language packages
ii chromium-codecs-ffmpeg 11.0.696.65~r84435-0ubuntu0.10.04.1 Free ffmpeg codecs for the Chromium Browser
ii cisco-auditing-tool 1.0-bt1 Perl script which scans cisco routers for common

vulnerabilities.
ii cisco-global-exploiter 13-bt1 Cisco Global Exploiter (CGE), is an advanced, simple and fast security testing tool.
ii cisco-ocs 0.1-bt3 Mass cisco scanner
ii cisco-torch 0.4-bt1 Cisco Scanner
ii ciscos 1.3-bt1 Cisco Scanner will scan a range of IP address for Cisco routers that havn't changed their default password of "cisco".
ii clamav-base 0.97.3+dfsg-1ubuntu1~lucid1~ppa1 anti-virus utility for Unix - base package
ii clamav-freshclam 0.97.3+dfsg-1ubuntu1~lucid1~ppa1 anti-virus utility for Unix - virus database update utility
ii cmospwd 5.0-bt0 Decrypts password stored in cmos used to access BIOS SETUP.
ii cms-explorer 1.0-bt2 CMS Explorer is designed to reveal the the specific modules, plugins, components and themes that various CMS driven web sites are running.
ii comerr-dev 2.1-1.41.11-1ubuntu2.1 common error description library - headers and static libraries
ii command-not-found 0.2.40ubuntu5 Suggest installation of packages in interactive bash sessions
ii command-not-found-data 0.2.40ubuntu5 Set of data files for command-not-found.
ii compiz 1:0.8.4-0ubuntu15.3 OpenGL window and compositing manager
ii compiz-core 1:0.8.4-0ubuntu15.3 OpenGL window and compositing manager
ii compiz-fusion-plugins-extra 0.8.4-0ubuntu2 Collection of extra plugins from OpenCompositing for Compiz
ii compiz-fusion-plugins-main 0.8.4-0ubuntu3 Collection of plugins from OpenCompositing for Compiz
ii compiz-gnome 1:0.8.4-0ubuntu15.3 OpenGL window and compositing manager - GNOME window decorator
ii compiz-plugins 1:0.8.4-0ubuntu15.3 OpenGL window and compositing manager - plugins
ii compizconfig-backend-gconf 0.8.4-0ubuntu2 Settings library for plugins - OpenCompositing Project
ii compizconfig-settings-manager 0.8.2-0ubuntu1 Compiz configuration settings manager
ii complemento 0.7.7.1-bt0 Complemento is a collection of tools for pentester: LetDown is a powerful 3-way-handshake tcp flooder ReverseRaider is a domain scanner that use wordlist
ii conky 1.8.0-1ubuntu1 highly configurable system monitor (transitional package)
ii conky-all 1.8.0-1ubuntu1 highly configurable system monitor (all features enabled)
ii console-setup 1.34ubuntu15 console font and keymap setup program
ii console-terminus 4.30-2 Fixed-width fonts for fast reading on the Linux console
ii consolekit 0.4.1-3ubuntu2 framework for defining and tracking users, sessions and seats
ii copy-router-config 4.0-bt3 Copy Cisco Router config - Using SNMP.
ii coreutils 7.4-2ubuntu3 The GNU core utilities
ii cowpatty 4.3-bt0 coWPAtty - Attacking WPA/WPA2-PSK Exchanges
ii cpio 2.10-1ubuntu2 GNU cpio -- a program to manage archives of files
ii cpp 4:4.4.3-1ubuntu1 The GNU C preprocessor (cpp)
ii cpp-4.4 4.4.3-4ubuntu5 The GNU C preprocessor
ii cpu-checker 0.1-0ubuntu2 tools to help evaluate certain CPU (or BIOS) features
ii creepy 0.1.93-bt1 creepy is an application that allows you to gather geolocation related information about users from social networking platforms and image hosting services
ii cron 3.0pl1-106ubuntu5 process scheduling daemon

ii crunch 3.0.1-bt0 Crunch is a wordlist generator where you can specify a standard character set or a character set you specify. crunch can generate all possible combination
ii cryptcat 1.2.1-bt2 Cryptcat is the standard netcat enhanced with twofish encryption.
ii cryptsetup 2:1.1.0~rc2-1ubuntu13 configures encrypted block devices
ii cupp 3.1-bt0 Common User Passwords Profiler
ii cups 1.4.3-1ubuntu1.4 Common UNIX Printing System(tm) - server
ii cups-bsd 1.4.3-1ubuntu1.4 Common UNIX Printing System(tm) - BSD commands
ii cups-client 1.4.3-1ubuntu1.4 Common UNIX Printing System(tm) - client programs (SysV)
ii cups-common 1.4.3-1ubuntu1.4 Common UNIX Printing System(tm) - common files
ii cups-driver-gutenprint 5.2.5-0ubuntu1.1 printer drivers for CUPS
ii cups-pdf 2.5.0-12 PDF printer for CUPS
ii cupsys 1.4.3-1ubuntu1.4 Common UNIX Printing System (transitional package)
ii cupsys-client 1.4.3-1ubuntu1.4 Common UNIX Printing System (transitional package)
ii curl 7.19.7-1ubuntu1 Get a file from an HTTP, HTTPS or FTP server
ii cve 1.0-bt1 Firefox link to Mitre-CVE.
ii cvs 1:1.12.13-12ubuntu1 Concurrent Versions System
ii cymothoa 1alpha-bt0 Cymothoa is a stealth backdooring tool, that inject backdoor's shellcode into an existing process.
ii darkmysqli 1.0-bt2 Multi-Purpose MySQL Injection Tool.
ii darkstat 3.0.713-bt0 Captures network traffic, calculates statistics about usage, and serves reports over HTTP. Traffic graphs, reports per host, shows ports for each host.
ii dash 0.5.5.1-3ubuntu2 POSIX-compliant shell
ii davtest 1.0-bt0 Tests WebDAV enabled servers by uploading test executable files.
ii dbconfig-common 1.8.44ubuntu1 common framework for packaging database applications
ii dbpwaudit 0.8-bt1 Java tool that allows you to perform online audits of password quality for several database engines
ii dbus 1.2.16-2ubuntu4.2 simple interprocess messaging system
ii dbus-x11 1.2.16-2ubuntu4.2 simple interprocess messaging system (X11 deps)
ii dc3dd 7.0.0-bt0 A patched version of GNU dd to include a number of features useful for computer forensics.
ii dcfldd 1.3.4.1-2 enhanced version of dd for forensics and security
ii ddrescue 1.14-bt0 Like dd, dd_rescue does copy data from one file or block device to another.
ii debconf 1.5.28ubuntu4 Debian configuration management system
ii debconf-i18n 1.5.28ubuntu4 full internationalization support for debconf
ii debhelper 7.4.15ubuntu1 helper programs for debian/rules
ii debianutils 3.2.2 Miscellaneous utilities specific to Debian
ii dedected 1.0-bt3 com_on_air_cs is a very basic driver for the Dosch & Amand com-on-air PCMCIA DECT cards.
ii default-jdk 1.6-34 Standard Java or Java compatible Development Kit
ii default-jre 1.6-34 Standard Java or Java compatible Runtime
ii default-jre-headless 1.6-34 Standard Java or Java compatible Runtime (headless)
ii defoma 0.11.10-4ubuntu1 Debian Font Manager -- automatic font configuration framework
ii desktop-file-utils 0.16-0ubuntu2 Utilities for .desktop files
ii devhelp 2.30.0-0ubuntu1 A GNOME developers help program
ii devhelp-common 2.30.0-0ubuntu1 common files for devhelp and its library

ii dff 1.1.0-bt0 DFF (Digital Forensics Framework) is a free and Open Source platform dedicated to digital forensic and eDiscovery sciences.
ii dh-make 0.50 tool that converts source archives into Debian package source
ii dhcp3-client 3.1.3-2ubuntu3.2 DHCP client
ii dhcp3-common 3.1.3-2ubuntu3.2 common files used by all the dhcp3* packages
ii dialog 1.1-20080819-1 Displays user-friendly dialog boxes from shell scripts
ii dictionaries-common 1.4.0ubuntu2 Common utilities for spelling dictionary tools
ii diffutils 1:2.8.1-18 File comparison utilities
ii dirbuster 0.12-bt2 DirBuster is a multi threaded java application designed to brute force directories and files names on web/application servers. Often is the case now of wh
ii dirmngr 1.0.3-1 server for managing certificate revocation lists
ii discover 2.1.2-3 hardware identification system
ii discover-data 2.2009.12.19 Data lists for Discover hardware detection system
ii discover1 2.1.2-3 transitional package
ii disktype 9-1 detection of content format of a disk or disk image
ii dkms 2.1.1.2-2fakesync1 Dynamic Kernel Module Support Framework
ii dmidecode 2.9-1.2 Dump Desktop Management Interface data
ii dmitry 1.3a-bt2 DMitry has the ability to gather as much information as possible about a host.
ii dmraid 1.0.0.rc16-3ubuntu2 Device-Mapper Software RAID support tool
ii dmsetup 2:1.02.39-1ubuntu4.1 The Linux Kernel Device Mapper userspace library
ii dnet-common 2.49ubuntu1 Base package for Linux DECnet
ii dns2tcp 0.5.2-bt1 Dns2tcp is a tool for relaying TCP connections over DNS.
ii dnsenum 1.2.2-bt0 dnsenum script for enumerating DNS servers
ii dnsmap 0.30-bt3 dnsmap is mainly meant to be used by pentesters during the information gathering/enumeration phase of infrastructure security assessments.
ii dnsrecon 0.5-bt0 DNS Enumeration Script
ii dnstracer 1.9-bt2 Dnstracer determines where a given Domain Name Server (DNS) gets its information from, and follows the chain of DNS servers back to the servers which know
ii dnsutils 1:9.7.0.dfsg.P1-1ubuntu0.1 Clients provided with BIND
ii dnswalk 2.0.2-bt1 dnswalk is a DNS debugger. It performs zone transfers of specifieddomains, and checks the database in numerous ways for internalconsistency, as well as ac
ii doc-base 0.9.5 utilities to manage online documentation
ii docbook-xml 4.5-7 standard XML documentation system for software and systems
ii docbook-xsl 1.75.2+dfsg-3 stylesheets for processing DocBook XML to various output formats
ii docbook-xsl-doc-html 1.75.2-1 stylesheets for processing DocBook XML files (HTML documentation)
ii dolphin 4:4.5.3-0ubuntu1~lucid1~ppa1 file manager for KDE 4
ii dos2unix 5.0-bt0 Includes utilities to convert text files with DOS or Mac line endings to Unix line endings.
ii dosfstools 3.0.7-1 utilities for making and checking MS-DOS FAT filesystems
ii doxygen 1.6.3-1 Documentation system for C, C++, Java, Python and other languages
ii dpkg 1.15.5.6ubuntu4.5 Debian package management system
ii dpkg-dev 1.15.5.6ubuntu4.5 Debian package development tools
ii dradis 2.7.0-bt3 Dradis is an open source framework to enable effective information sharing, specially during security assessments.

ii driftnet 0.1.6-bt2 A program which listens to network traffic and picks out images.
ii dsniff 2.4b1-bt1 A collection of tools for network auditing and penetration testing.
ii dvd+rw-tools 7.1-6 DVD+-RW/R tools
ii dvdauthor 0.6.14-3ubuntu4 create DVD-Video file system
ii dvgrab 3.5-1 grab digital video data via IEEE1394 and USB links
ii e2fslibs 1.41.11-1ubuntu2.1 ext2/ext3/ext4 file system libraries
ii e2fsprogs 1.41.11-1ubuntu2.1 ext2/ext3/ext4 file system utilities
ii eapmd5pass 1.4-bt0 An implementation of an offline dictionary attack against the EAP-MD5 protocol.
ii easytag 2.1.6-1ubuntu1 viewing, editing and writing ID3 tags
ii eclipse 3.5.2-2ubuntu4.3 Extensible Tool Platform and Java IDE
ii eclipse-jdt 3.5.2-2ubuntu4.3 Eclipse Java Development Tools (JDT)
ii eclipse-pde 3.5.2-2ubuntu4.3 Eclipse Plug-in Development Environment (PDE)
ii eclipse-platform 3.5.2-2ubuntu4.3 Eclipse platform without plug-ins to develop any language
ii eclipse-platform-data 3.5.2-2ubuntu4.3 Eclipse platform without plug-ins to develop any language (data)
ii eclipse-plugin-cvs 3.5.2-2ubuntu4.3 Eclipse Team Integration (CVS support)
ii eclipse-rcp 3.5.2-2ubuntu4.3 Eclipse Rich Client Platform (RCP)
ii ecryptfs-utils 83-0ubuntu3.1 ecryptfs cryptographic filesystem (utilities)
ii ed 1.4-1build1 The classic UNIX line editor
ii edb-debugger 0.9.17-bt4 Evans Debugger, GUI debugger for linux x86 and x64.
ii eject 2.1.5+deb1+cvs20081104-7 ejects CDs and operates CD-Changers under Linux
ii elinks 0.12~pre5-2ubuntu1 advanced text-mode WWW browser
ii elinks-data 0.12~pre5-2ubuntu1 advanced text-mode WWW browser - data files
ii enigmail 2:1.1.2-0ubuntu0.10.04.1 GPG support for Thunderbird and Debian Icedove
ii enumiax 1.0-bt3 enumIAX is an Inter Asterisk Exchange version 2 (IAX2) protocol username brute-force enumerator. enumIAX may operate in two distinct modes; Sequential Use
ii esound-clients 0.2.41-6ubuntu1 Enlightened Sound Daemon - clients
ii esound-common 0.2.41-6ubuntu1 Enlightened Sound Daemon - Common files
ii eterm 0.9.5-2ubuntu1 Enlightened Terminal Emulator
ii etherape 0.9.8-1 graphical network monitor modeled after etherman
ii ethtool 6+20091202-1 display or change Ethernet device settings
ii ettercap-common 1:0.7.3-1.4ubuntu1 Common support files and plugins for ettercap
ii ettercap-desktop 0.7.3-bt2 Multipurpose sniffer/interceptor/logger for switched LAN.
ii ettercap-gtk 1:0.7.3-1.4ubuntu1 Multipurpose sniffer/interceptor/logger for switched LAN
ii evince 2.30.3-0ubuntu1.2 Document (postscript, pdf) viewer
ii evtparse.pl 1.0-bt0 Script to parse Windows 2000/XP/2003 Event Log files.
ii ewf-tools 20100119-1 collection of tools for reading and writing EWF files
ii ewfacquire 20100119-bt1 Use ewfacquire to acquire data from a file or device and store it in the EWF format.
ii exif 0.6.19-1 command-line utility to show EXIF information in JPEG files
ii exiftool 8.56-bt0 ExifTool is a platform-independent Perl library plus a command-line application for reading, writing and editing meta information in a wide variety of fil
ii exiv2 0.19-1 EXIF/IPTC metadata manipulation tool
ii expat 2.0.1-7ubuntu1 XML parsing C library - example application

ii exploitdb 2.0-bt0 A SVN archive of the exploit-db.
ii extract 0.5.23+dfsg-4build1 displays meta-data from files of arbitrary type
ii fakeroot 1.14.4-1ubuntu1 Gives a fake root environment
ii fancontrol 1:3.1.2-2 utilities to read temperature/voltage/fan sensors
ii farpd 0.2-10 Fake ARP user space daemon
ii fastjar 2:0.98-1ubuntu0.10.04.1 Jar creation utility
ii fasttrack 4.0.2-bt0 Fast-Track is an exploitation framework used to automated penetration testing efforts.
ii fatback 1.3-bt2 A *nix tool for recovering files from FAT file systems.
ii fatresize 1.0.2-4ubuntu2 FAT16/FAT32 filesystem resizer
ii fcrackzip 1.0-bt1 fcrackzip is a zip password cracker, similar to fzc, zipcrack and others.
ii feh 1.3.4.dfsg.1-3 imlib2 based image viewer
ii ferret 2.0-bt2 Ferret is a tool for sniffing and analyzing packets and pulling out
ii festival 1.96~beta-10ubuntu1 General multi-lingual speech synthesis system
ii festlex-cmu 1.4.0-6 CMU dictionary for Festival
ii festlex-poslex 1.4.0-5 Part of speech lexicons and ngram from English
ii festvox-kallpc16k 1.4.0-5 American English male speaker for festival, 16khz sample rate
ii ffmpeg 4:0.5.1-1ubuntu1.1 multimedia player, server and encoder
ii fierce 0.9.9-bt4 Fierce is a PERL script that quickly scans domains.
ii figlet 2.2.2-1ubuntu1 Frank, Ian & Glenn's Letters
ii fiked 0.0.5-bt0 FakeIKEd, or fiked for short, is a fake IKE daemon supporting just enough of the standards and Cisco extensions to attack commonly found insecure Cisco VP
ii file 5.03-5ubuntu1 Determines file type using "magic" numbers
ii filezilla 3.3.1-1ubuntu2 Full-featured graphical FTP/FTPS/SFTP client
ii filezilla-common 3.3.1-1ubuntu2 Architecture independent files for filezilla
ii fimap 0.8.1-bt2 fimap is a little python tool which can find, prepare, audit, exploit and even google automaticly for local and remote file inclusion bugs in webapps.
ii findutils 4.4.2-1ubuntu1 utilities for finding files--find, xargs
ii firebird2.1-common 2.1.3.18185-0.ds1-6build1 common files for firebird 2.1 servers and clients
ii firebird2.1-common-doc 2.1.3.18185-0.ds1-6build1 copyright, licensing and changelogs of firebird2.1
ii firefox 9.0.1-bt0 Firefox web browser
ii firefox-user-profile 1.0-bt2 Firefox profile
ii flashplugin-installer 10.2.159.1ubuntu0.10.04.1 Adobe Flash Player plugin installer
ii flashplugin-nonfree 10.2.159.1ubuntu0.10.04.1 Adobe Flash Player plugin installer (transitional package)
ii flashplugin-nonfree-extrasound 0.0.svn2431-3 Adobe Flash Player platform support library for Esound and OSS
ii flasm 1.62-bt0 Flash disasembler
ii flex 2.5.35-9 A fast lexical analyzer generator.
ii fontconfig 2.8.0-2ubuntu1 generic font configuration library - support binaries
ii fontconfig-config 2.8.0-2ubuntu1 generic font configuration library - configuration
ii foo2zjs 20100210-0ubuntu4 Support for printing to ZjStream-based printers
ii foomatic-db 20100216-0ubuntu3 OpenPrinting printer support - database
ii foomatic-db-engine 4.0.4-0ubuntu1 OpenPrinting printer support - programs
ii foomatic-db-gutenprint 5.2.5-0ubuntu1.1 OpenPrinting printer support - database for Gutenprint printer drivers

ii foomatic-filters 4.0.4-0ubuntu1 OpenPrinting printer support - filters
ii foremost 1.5.7-bt0 A console program to recover files based on their headers, footers, and internal data structures.
ii fortune-mod 1:1.99.1-3.1ubuntu4 provides fortune cookies on demand
ii fortunes-min 1:1.99.1-3.1ubuntu4 Data files containing fortune cookies
ii fotoxx 8.7-1 easy-to-use digital photo editor
ii fping 2.4b2-bt0 A ping-like program which uses the Internet Control Message Protocol (ICMP) echo request to determine if a host is up.
ii fragroute 1.2-bt1 fragroute intercepts, modifies, and rewrites egress traffic destined for a specified host
ii fragrouter 1.6-bt3 Fragrouter is a network intrusion detection evasion toolkit.
ii framework 4.0.0-bt1 The Metasploit exploitation framework
ii framework2 2.8-bt0 A powerful exploitation framework.
ii framework3 3.7.2-bt2 Metasploit Exploitation Framework
ii freeradius-wpe 2.1.7-bt1 A patch for the popular open-source FreeRADIUS implementation to demonstrate RADIUS impersonation vulnerabilities by Joshua Wright and Brad Antoniewicz, d
ii freetds-common 0.82-6build1 configuration files for FreeTDS SQL client libraries
ii frei0r-plugins 1.1.22git20090409+repack-0ubuntu3 minimalistic plugin API for video effects, plugins collection
ii friendly-recovery 0.2.10 Make recovery more user-friendly
ii fsarchiver 0.6.8-1ubuntu0.1 file system archiver
ii ftester 1.0-bt0 A tool designed for testing firewall filtering policies and Intrusion Detection System (IDS) capabilities.
ii ftp 0.17-19build1 The FTP client
ii funkload 1.16.0-bt0 FunkLoad is a functional and load web tester, written in Python
ii fuse-utils 2.8.1-1.1ubuntu3.1 Filesystem in USErspace (utilities)
ii fuseiso 20070708-1 FUSE module to mount ISO filesystem images
ii fusion-icon 0.1.0-2 tray icon to launch and manage Compiz Fusion
ii fvwm1 1.24r-54 Old version of the F(?) Virtual Window Manager
ii g++ 4:4.4.3-1ubuntu1 The GNU C++ compiler
ii g++-4.4 4.4.3-4ubuntu5 The GNU C++ compiler
ii galleta 1.0+20040505-5 An Internet Explorer cookie forensic analysis tool
ii gamin 0.1.10-1ubuntu3 File and directory monitoring system
ii gap-character-tables 1r1p3-5 GAP Library of character tables
ii gawk 1:3.1.6.dfsg-4build1 GNU awk, a pattern scanning and processing language
ii gcalctool 5.30.0.is.5.28.2-0ubuntu2 GNOME desktop calculator
ii gcc 4:4.4.3-1ubuntu1 The GNU C compiler
ii gcc-4.4 4.4.3-4ubuntu5 The GNU C compiler
ii gcc-4.4-base 4.4.3-4ubuntu5 The GNU Compiler Collection (base package)
ii gcj-4.4-base 4.4.3-1ubuntu4.1 The GNU Compiler Collection (gcj base package)
ii gcj-4.4-jre-lib 4.4.3-1ubuntu4.1 Java runtime library for use with gcj (jar files)
ii gconf2 2.28.1-0ubuntu1 GNOME configuration database system (support tools)
ii gconf2-common 2.28.1-0ubuntu1 GNOME configuration database system (common files)
ii gdb 7.1-1ubuntu2 The GNU Debugger
ii gdebi-core 0.6.0ubuntu2 Simple tool to install deb files
ii gdebi-kde 0.6.0ubuntu2 Simple tool to install deb files - KDE GUI
ii geany 0.18-1 A fast and lightweight IDE

ii genisoimage 9:1.1.10-1ubuntu1 Creates ISO-9660 CD-ROM filesystem images
ii geoip-database 1.4.6.dfsg-17 IP lookup command line tools that use the GeoIP library (country database)
ii gerix-wifi-cracker-ng 2.0-bt2 Aicrack-NG (WPA/WEP) GUI with pyrit support on cracking
ii getsids 0.0.1-bt2 Tries to enumerate Oracle Sids by sending the services command to the Oracle TNS listener.
ii gettext 0.17-8ubuntu3 GNU Internationalization utilities
ii gettext-base 0.17-8ubuntu3 GNU Internationalization utilities for the base system
ii gfxboot 3.3.39-0ubuntu4 bootlogo creator for gfxboot compliant boot loaders
ii ghdb 1.0-bt1 Firefox link to GHDB.
ii ghex 2.24.0-1 GNOME Hex editor for files
ii ghostscript 8.71.dfsg.1-0ubuntu5.3 The GPL Ghostscript PostScript/PDF interpreter
ii ghostscript-cups 8.71.dfsg.1-0ubuntu5.3 The GPL Ghostscript PostScript/PDF interpreter - CUPS filters
ii giblib1 1.2.4-5 wrapper library for imlib2, and other stuff
ii gimp 2.6.8-2ubuntu1.2 The GNU Image Manipulation Program
ii gimp-data 2.6.8-2ubuntu1.2 Data files for GIMP
ii giskismet 1.0-bt2 GISKismet is a wireless recon visualization tool to represent data gathered using Kismet in a flexible manner. GISKismet stores the information in a datab
ii git-core 1:1.7.0.4-1ubuntu0.2 fast, scalable, distributed revision control system
ii gkamus 1.0-1 Package created with checkinstall 1.6.1
ii gksu 2.0.2-2ubuntu2 graphical frontend to su
ii globalplatform 6.0.0-bt0 The GlobalPlatform card specification is a standard for the management of the contents on a smart card. Mainly this comprises the installation and the rem
ii gnome-doc-utils 0.20.0-0ubuntu2 a collection of documentation utilities for the GNOME project
ii gnome-extra-icons 1.1-2 Optional GNOME icons
ii gnome-icon-theme 2.28.0-1ubuntu1 GNOME Desktop icon theme
ii gnome-keyring 2.92.92.is.2.30.3-0ubuntu1.1 GNOME keyring services (daemon and tools)
ii gnome-mime-data 2.18.0-1 base MIME and Application database for GNOME.
ii gnome-user-guide 2.30.0+git20100403ubuntu2 GNOME user's guide
ii gnupg 1.4.10-2ubuntu1 GNU privacy guard - a free PGP replacement
ii gnupg-agent 2.0.14-1ubuntu1.2 GNU privacy guard - password agent
ii gnupg-curl 1.4.10-2ubuntu1 GNU privacy guard - a free PGP replacement (cURL)
ii gnupg2 2.0.14-1ubuntu1.2 GNU privacy guard - a free PGP replacement (new v2.x)
ii gnuplot 4.2.6-1 A command-line driven interactive plotting program
ii gnuplot-nox 4.2.6-1 A command-line driven interactive plotting program
ii gnuplot-x11 4.2.6-1 A command-line driven interactive plotting program
ii gocr 0.46-2.1 A command line OCR
ii goohost 0.0.1-bt1 Simple script that extracts hosts/subdomains, ip or emails for a specific domain with Google search.
ii gooscan 1.0-bt2 Gooscan is a tool developed by Johny Long. It automates queries against Google search appliances with the goal to identify vulnerabilities on web sites.
ii gparted 0.5.1-1ubuntu3 GNOME partition editor
ii gpgsm 2.0.14-1ubuntu1.2 GNU privacy guard - S/MIME version
ii gpgv 1.4.10-2ubuntu1 GNU privacy guard - signature verification tool
ii gpsd 2.92-4 Global Positioning System - daemon

ii gpshell 1.4.4-bt0 GPshell for Globalplatform
ii grabber 0.1-bt1 Grabber is a web application scanner.
ii graphviz 2.20.2-8ubuntu3 rich set of graph drawing tools
ii greenbone-security-assistant 2.0.1-bt8 The Greenbone Security Assistant is a web application that connects to the OpenVAS Manager and OpenVAS Administrator to provide for a full-featured user i
ii greenbone-security-desktop 1.2.0-bt0 The GSD is a desktop client that connects to the OpenVAS Manager using the OMP protocol.
ii grendel-scan 1.0-bt1 Grendel-Scan is an open-source web application security testing tool.
ii grep 2.5.4-4build1 GNU grep, egrep and fgrep
ii groff 1.20.1-7 GNU troff text-formatting system
ii groff-base 1.20.1-7 GNU troff text-formatting system (base system components)
ii grub-common 1.98-1ubuntu12 GRand Unified Bootloader, version 2 (common files)
ii grub-pc 1.98-1ubuntu12 GRand Unified Bootloader, version 2 (PC/BIOS version)
ii gsfonts 1:8.11+urwcyr1.0.7~pre44-4 Fonts for the Ghostscript interpreter(s)
ii gsfonts-x11 0.21 Make Ghostscript fonts available to X11
ii gstm 1.2-7ubuntu1 SSH tunnel manager for GNOME
ii gstreamer0.10-alsa 0.10.28-1 GStreamer plugin for ALSA
ii gstreamer0.10-doc 0.10.28-1 GStreamer core documentation and manuals
ii gstreamer0.10-ffmpeg 0.10.10-1 FFmpeg plugin for GStreamer
ii gstreamer0.10-gnonlin 0.10.15-1 non-linear editing module for GStreamer
ii gstreamer0.10-nice 0.0.10-2build1 ICE library (GStreamer plugin)
ii gstreamer0.10-plugins-base 0.10.28-1 GStreamer plugins from the "base" set
ii gstreamer0.10-plugins-good 0.10.21-1ubuntu3 GStreamer plugins from the "good" set
ii gstreamer0.10-plugins-ugly 0.10.14-1 GStreamer plugins from the "ugly" set
ii gstreamer0.10-x 0.10.28-1 GStreamer plugins for X11 and Pango
ii gtk-recordmydesktop 0.3.8-1ubuntu1 Graphical frontend for recordmydesktop screencast tool
ii gtk2-engines-pixbuf 2.20.1-0ubuntu2 Pixbuf-based theme for GTK+ 2.x
ii gtkdialog 2:0.8.0 GUI-creation command-line utility based on GTK+ library
ii gtklp 1.2.7-2 printing tool for CUPS on the GNOME Desktop
ii gtypist 2.8.3-1 A simple ncurses touch typing tutor
ii gummi 0.6.11~lucid-1 Simple LaTeX editor for Linux
ii gvfs 1.6.1-0ubuntu1build1 userspace virtual filesystem - server
ii gvfs-backends 1.6.1-0ubuntu1build1 userspace virtual filesystem - backends
ii gvfs-bin 1.6.1-0ubuntu1build1 userspace virtual filesystem - binaries
ii gwenview 4:4.5.3-0ubuntu1~lucid1~ppa1 image viewer for KDE 4
ii gzip 1.3.12-9ubuntu1.1 GNU compression utilities
ii hack-library 1.0-bt2 A collection of tools used for SIP attack tools.
ii hal 0.5.14-0ubuntu6 Hardware Abstraction Layer
ii hal-info 20091130-1 Hardware Abstraction Layer - fdi files
ii hamster 2.0-bt2 Sidejacking tool which, when used with ferret can steal and replay session cookies
ii hashcat 0.38-bt0 cpu based multihash cracker
ii hashcat-utils 0.5-bt0 Utilities for creating and manipulation wordlists
ii hdparm 9.15-1ubuntu9 tune hard disk parameters for high performance
ii hexedit 1.2.12-bt0 View and edit files in hexadecimal or in ASCII.

ii hexer 0.1.5-1 An interactive binary editor with a Vi-like interface
ii hexinject 1.4-bt0 HexInject is a very versatile packet injector and sniffer, that provide a command-line framework for raw network access.
ii hicolor-icon-theme 0.11-1 default fallback theme for FreeDesktop.org icon themes
ii honeycomb 0.7-bt6 Automated signature creation using honeypots.
ii honeyd 1.5c-bt3 Honeyd is a small daemon that creates virtual hosts on a network.
ii hostname 3.03ubuntu1 utility to set/show the host name or domain name
ii hotot 2:0.9.7~git-1301-g830ffe8-0ubuntu0ppa1~lucid1 Lightweight Twitter Client based on GTK2 and Webkit.
ii hpijs 3.10.2-2ubuntu2.2 HP Linux Printing and Imaging - gs IJS driver (hpijs)
ii hping2 2.0.0-rc3-bt2 hping is a command-line oriented TCP/IP packet assembler/analyzer.
ii hping3 20051105-bt2 hping is a command-line oriented TCP/IP packet assembler/analyzer. The interface is inspired to the ping(8) unix command, but hping isn't only able to sen
ii html2text 1.3.2a-14build1 advanced HTML to text converter
ii htmldoc 1.8.27-4.1 HTML processor that generates indexed HTML, PS, and PDF
ii htmldoc-common 1.8.27-4.1 Common arch-independent files for htmldoc
ii httprint 301-bt2 httprint is a web server fingerprinting tool. It relies on web server characteristics to accurately identify web servers, despite the fact that they may h
ii httrack 3.43.9-1ubuntu1 Copy websites to your computer (Offline browser)
ii hunspell-ar 0.0.0+20080110-1.1 Arabic dictionary for hunspell
ii hunspell-en-ca 1:3.2.0-3ubuntu3.1 English_canadian dictionary for hunspell
ii hunspell-en-us 20070829-4ubuntu1 English_american dictionary for hunspell
ii hydra 7.1-bt0 A very fast network logon cracker which support many different services.
ii iat 0.1.3-7 Converts many CD-ROM image formats to iso9660
ii iaxflood 1.0-bt0 A UDP Inter-Asterisk_eXchange (i.e. IAX)
ii ibus 1.2.0.20091215-1ubuntu4 New input method framework using dbus
ii ibus-anthy 1.2.0.20100115-1ubuntu0.1 anthy engine for IBus
ii ibus-gtk 1.2.0.20091215-1ubuntu4 New input method framework using dbus
ii icedtea-6-jre-cacao 6b20-1.9.7-0ubuntu1~10.04.1 Alternative JVM for OpenJDK, using Cacao
ii icoutils 0.29.1-0ubuntu1~lucid Create and extract MS Windows icons and cursors
ii ida-pro-free 5.0-bt3 The IDA Pro Disassembler and Debugger is an interactive, programmable, extendible, multi-processor disassembler hosted on Windows, Linux, or Mac OS X.
ii ifdokrfid 2.8.1-bt3 Omnikey Drivers
ii ifupdown 0.6.8ubuntu29.2 high level tools to configure network interfaces
ii iisemulator 0.95-3 Emulation for the IIS web server
ii ijsgutenprint 5.2.5-0ubuntu1.1 inkjet server - Ghostscript driver for Gutenprint
ii ike-scan 1.9-bt2 ike-scan is a command-line tool that uses the IKE protocol to discover, fingerprint and test IPsec VPN servers.
ii im-switch 1.19 Input method switch framework
ii imagemagick 7:6.5.7.8-1ubuntu1.1 image manipulation programs
ii impacket-examples 0.9.6.0-bt1 A collection of Python classes focused on providing access to network packets.
ii indicator-application 0.0.19-0ubuntu4 Application Indicators
ii info 4.13a.dfsg.1-5ubuntu1 Standalone GNU Info documentation browser

ii initramfs-tools 0.92bubuntu78 tools for generating an initramfs
ii initramfs-tools-bin 0.92bubuntu78 binaries used by initramfs-tools
ii initscripts 2.87dsf-4ubuntu17.2 scripts for initializing and shutting down the system
ii inkscape 0.47.0-2ubuntu2 vector-based drawing program
ii insserv 1.12.0-14 Tool to organize boot sequence using LSB init.d script dependencies
ii install-info 4.13a.dfsg.1-5ubuntu1 Manage installed documentation in info format
ii install-package 0.5.2 Install a package GUI
ii installation-report 2.39ubuntu4 system installation report
ii intel-gpu-tools 1.0.2+git20100324-0ubuntu1 tools for debugging the Intel graphics driver
ii intltool 0.41.0-0ubuntu1 Utility scripts for internationalizing XML
ii intltool-debian 0.35.0+20060710.1 Help i18n of RFC822 compliant config files
ii inviteflood 2.0-bt1 Command line tool to attempt to flood a specific destination.
ii iodine 0.6.0-rc1-bt2 This is a piece of software that lets you tunnel IPv4 data through a DNS server. This can be usable in different situations where internet access is firew
ii ipcalc 0.41-bt1 IPv4 Calculator
ii iproute 20091226-1 networking and traffic control tools
ii ipscan 3.0-beta6-1 Angry IP Scanner - fast and friendly IP Scanner
ii iptables 1.4.4-2ubuntu2 administration tools for packet filtering and NAT
ii iptraf 3.0.0-7ubuntu0.10.04 Interactive Colorful IP LAN Monitor
ii iputils-arping 3:20071127-2ubuntu1 Tool to send ARP Requests for an IP address
ii iputils-ping 3:20071127-2ubuntu1 Tools to test the reachability of network hosts
ii iputils-tracepath 3:20071127-2ubuntu1 Tools to trace the network path to a remote host
ii irb 4.2-2~uorppa0 Interactive Ruby (irb)
ii irb1.8 1.8.7.249-2 Interactive Ruby (for Ruby 1.8)
ii irb1.9.2 1.9.2.z1-1ppa1~lucid Interactive Ruby (for Ruby 1.9.2)
ii irpas 0.10-bt1 The idea is to implement small tools which can be scripted for larger tests while using the protocols describd in standards or white papers. IRPAS is not
ii irqbalance 0.55+20091017-3ubuntu2 Daemon to balance interrupts for SMP systems
ii iso-codes 3.12.1-1 ISO language, territory, currency, script codes and their translations
ii isr-evilgrade 2.0.0-bt0 ISR Evilgrade is a modular framework that allow us to take advantage of poor upgrade implementations by injecting fake updates.
ii istanbul 0.2.2-6ubuntu1 Desktop session recorder producing Ogg Theora video
ii iw 0.9.22-bt2 iw is a new nl80211 based CLI configuration utility for wireless devices.
ii iwar 0.08-bt1 iWar is a "war dialer" written completely in C for Unix types of operating systems (Linux, FreeBSD, OpenBSD, etc). It is intended for legal phone security
ii jarwrapper 0.37ubuntu1~lucid1 Run executable Java .jar files
ii java-common 0.34 Base of all Java packages
ii javascript-common 7 Base support for javascript library packages
ii john 1.7.8-jumbo-8-bt1 John the Ripper is a fast password cracker. Besides several crypt(3) password hash types most commonly found on various Unix flavors, supported out of the
ii joomscan 0.0.4-bt3 Detects file inclusion, sql injection, command execution vulnerabilities of a target Joomla! web site.
ii junit 3.8.2-4 Automated testing framework for Java
ii junit4 4.8.1-3 JUnit regression test framework for Java
ii k3b 2.0.1-1ubuntu3~lucid1~ppa1 A sophisticated CD/DVD burning application
ii k3b-data 2.0.1-1ubuntu3~lucid1~ppa1 A sophisticated CD/DVD burning application - data files

ii kate 4:4.5.3-0ubuntu1~lucid1~ppa1 KDE 4 Advanced Text Editor
ii kbd 1.15-1ubuntu3 Linux console font and keytable utilities
ii kcalc 4:4.5.3-0ubuntu1~lucid1~ppa1 calculator for KDE 4
ii kcharselect 4:4.5.3-0ubuntu1~lucid1~ppa1 special character utility for KDE 4
ii kchmviewer 4.1-1 CHM viewer for KDE
ii kde-minimal 5:55ubuntu1 the K Desktop Environment, minimal applications
ii kde-window-manager 4:4.5.3-0ubuntu1~lucid1~ppa1 the KDE 4 window manager (KWin)
ii kdebase 5:55ubuntu1 the K Desktop Environment, base applications
ii kdebase-apps 4:4.5.3-0ubuntu1~lucid1~ppa1 base applications from the official KDE release
ii kdebase-bin 4:4.5.3-0ubuntu1~lucid1~ppa1 core binaries for the KDE 4 base module
ii kdebase-data 4:4.5.3-0ubuntu1~lucid1~ppa1 shared data files for the KDE 4 base module
ii kdebase-runtime 4:4.5.3-0ubuntu1~lucid1~ppa1 runtime components from the official KDE 4 release
ii kdebase-runtime-data 4:4.5.3-0ubuntu1~lucid1~ppa1 shared data files for the KDE 4 base runtime module
ii kdebase-workspace 4:4.5.3-0ubuntu1~lucid1~ppa1 base workspace components from the official KDE 4 release
ii kdebase-workspace-bin 4:4.5.3-0ubuntu1~lucid1~ppa1 core binaries for the KDE 4 base workspace module
ii kdebase-workspace-data 4:4.5.3-0ubuntu1~lucid1~ppa1 shared data files for the KDE 4 base workspace module
ii kdebase-workspace-kgreet-plugins 4:4.5.3-0ubuntu1~lucid1~ppa1 KDE greet libraries for authentication
ii kdebase-workspace-wallpapers 4:4.5.3-0ubuntu1~lucid1~ppa1 set of extra wallpapers from the KDE 4 base module
ii kdegraphics-libs-data 4:4.5.3-0ubuntu1~lucid1~ppa1 data files for libraries from the kdegraphics module
ii kdelibs-bin 4:4.5.3-0ubuntu1~lucid1~ppa2 core executables for KDE Aapplications
ii kdelibs-data 4:3.5.10.dfsg.1-3ubuntu2.10.04.1 core shared data for all KDE applications
ii kdelibs4c2a 4:3.5.10.dfsg.1-3ubuntu2.10.04.1 core libraries and binaries for all KDE applications
ii kdelibs5 4:4.5.3-0ubuntu1~lucid1~ppa2 transitional package for the KDE Development Platform libraries
ii kdelibs5-data 4:4.5.3-0ubuntu1~lucid1~ppa2 core shared data for all KDE Applications
ii kdelibs5-plugins 4:4.5.3-0ubuntu1~lucid1~ppa2 core plugins for KDE Applications
ii kdenlive 0.7.7.1-0ubuntu1 a non-linear video editor
ii kdenlive-data 0.7.7.1-0ubuntu1 a non-linear video editor (data files)
ii kdepasswd 4:4.5.3-0ubuntu1~lucid1~ppa1 password changer for KDE 4
ii kdepim-runtime 4:4.4.8-0ubuntu0.0.1 Runtime components for akonadi-kde
ii kdepimlibs-kio-plugins 4:4.5.3-0ubuntu1~lucid1~ppa1 kio slaves used by KDE PIM applications
ii kdepimlibs5 4:4.5.3-0ubuntu1~lucid1~ppa1 the KDE Development Platform PIM libraries (transitional package)
ii kdeplasma-addons 4:4.5.3-0ubuntu1~lucid1~ppa1 addons for KDE 4 Plasma - metapackage
ii kdesudo 3.4.2.3-0ubuntu1.1 sudo frontend for KDE4
ii kdewallpapers 4:4.5.3-0ubuntu1~lucid1~ppa1 wallpapers released with KDE

ii kdm 4:4.5.3-0ubuntu1~lucid1~ppa1 KDE Display Manager for X11
ii kdoctools 4:4.5.3-0ubuntu1~lucid1~ppa2 various tools for accessing application documentation
ii keepassx 0.4.3-1 Cross Platform Password Manager
ii keepnote 0.7.1-bt0 A note taking and organization application.
ii keimpx 0.2-bt0 It can be used to quickly check for the usefulness of credentials across a network over SMB.
ii kernel-package 12.032 A utility for building Linux kernel related Debian packages.
ii keyutils 1.2-12 Linux Key Management Utilities
ii kfind 4:4.5.3-0ubuntu1~lucid1~ppa1 file search utility for KDE 4
ii kgpg 4:4.5.3-0ubuntu1~lucid1~ppa1 encryption utility for KDE 4
ii kinfocenter 4:4.5.3-0ubuntu1~lucid1~ppa1 system information viewer for KDE
ii kino 1.3.4-1ubuntu1 Non-linear editor for Digital Video data
ii kismet 201103r2-bt1 An 802.11 layer2 wireless network detector, sniffer, and intrusion detection system.
ii kleopatra 4:4.4.8-0ubuntu0.0.1 KDE Certificate Manager
ii klibc-utils 1.5.17-4ubuntu1 small utilities built with klibc for early boot
ii klipper 4:4.5.3-0ubuntu1~lucid1~ppa1 clipboard utility for KDE 4
ii kmix 4:4.5.3-0ubuntu1~lucid1~ppa1 volume control and mixer for KDE
ii kmplot 4:4.5.3-0ubuntu1~lucid1~ppa3 mathematical function plotter for KDE
ii konqueror 4:4.5.3-0ubuntu1~lucid1~ppa1 KDE 4's advanced file manager, web browser and document viewer
ii konqueror-nsplugins 4:4.5.3-0ubuntu1~lucid1~ppa1 Netscape plugin support for Konqueror
ii konsole 4:4.5.3-0ubuntu1~lucid1~ppa1 X terminal emulator for KDE 4
ii kpackagekit 0.5.4-0ubuntu4.4~lucid1~ppa1 KDE package management tool using PackageKit
ii kradio 4.0.0-0ubuntu3 Comfortable Radio Application for KDE
ii krb5-multidev 1.8.1+dfsg-2ubuntu0.9 Development files for MIT Kerberos without Heimdal conflict
ii krosspython 4:4.5.3-0ubuntu1~lucid1~ppa5 Python module for Kross
ii ksnapshot 4:4.5.3-0ubuntu1~lucid1~ppa1 screen capture tool for KDE 4
ii ksysguard 4:4.5.3-0ubuntu1~lucid1~ppa1 System Guard for KDE 4
ii ksysguardd 4:4.5.3-0ubuntu1~lucid1~ppa1 System Guard Daemon for KDE 4
ii ktorrent 4.0.3-0ubuntu1~lucid1~ppa1 BitTorrent client based on the KDE platform
ii ktorrent-data 4.0.3-0ubuntu1~lucid1~ppa1 KTorrent data and other architecture independent files
ii ktouch 4:4.5.3-0ubuntu1~lucid1~ppa3 touch typing tutor for KDE
ii kubuntu-debug-installer 10.04ubuntu4 Debug package installer for Kubuntu
ii kvkbd 1:0.6-2ubuntu1 Virtual keyboard for KDE
ii kworldclock 4:3.5.9-2 earth watcher for KDE
ii kwrite 4:4.5.3-0ubuntu1~lucid1~ppa1 text editor for KDE 4
ii lacheck 1.26-11.1build1 A simple syntax checker for LaTeX
ii lame 3.98.2+debian-0ubuntu3 An MP3 encoding library (frontend)
ii landscape-common 11.02-0ubuntu0.10.04.1 The Landscape administration system client
ii language-pack-ar 1:10.04+20110204 translation updates for language Arabic
ii language-pack-ar-base 1:10.04+20110204 translations for language Arabic
ii language-pack-en 1:10.04+20110204 translation updates for language English

ii language-pack-en-base 1:10.04+20110204 translations for language English
ii language-pack-ja 1:10.04+20110204 translation updates for language Japanese
ii language-pack-ja-base 1:10.04+20110204 translations for language Japanese
ii language-selector-common 0.5.8 Language selector for Ubuntu Linux
ii language-support-ar 1:9.10+20090909 metapackage for Arabic language support
ii language-support-en 1:9.10+20090909 metapackage for English language support
ii language-support-fonts-ar 1:9.10+20090909 Additional fonts metapackage for Arabic
ii language-support-fonts-ja 1:10.04+20100420 Additional fonts metapackage for Japanese
ii language-support-input-ar 1:9.10+20090909 Input methods metapackage for Arabic
ii language-support-input-ja 1:9.10+20090915 Input methods metapackage for Japanese
ii language-support-ja 1:9.10+20090909 metapackage for Japanese language support
ii language-support-writing-ar 1:9.10+20090909 Writing aids metapackage for Arabic
ii language-support-writing-en 1:10.04+20100311 Writing aids metapackage for English
ii lanmap2 1.0-bt1 Builds database/visualizations of LAN structure from passively sifted information.
ii laptop-detect 0.13.7ubuntu2 attempt to detect a laptop
ii latex-beamer 3.07-2ubuntu1 LaTeX class to produce presentations
ii latex-xcolor 2.11-1 Easy driver-independent TeX class for color
ii launchpad-integration 0.1.35 launchpad integration
ii lbd 0.2-bt2 lbd (load balancing detector) detects if a given domain uses DNS and/or HTTP Load-Balancing.
ii less 436-1 pager program similar to more
ii lesstif2 1:0.95.2-1 OSF/Motif 2.1 implementation released under LGPL
ii liba52-0.7.4 0.7.4-13ubuntu1 library for decoding ATSC A/52 streams
ii libaa1 1.4p5-38build1 ascii art library
ii libaccess-bridge-java 1.26.2-3 Java Access Bridge for GNOME
ii libaccess-bridge-java-jni 1.26.2-3 Java Access Bridge for GNOME (jni bindings)
ii libacl1 2.2.49-2 Access control list shared library
ii libaio1 0.3.107-3ubuntu2 Linux kernel AIO access library - shared library
ii libakonadi-contact4 4:4.5.3-0ubuntu1~lucid1~ppa1 library for using the Akonadi PIM data server
ii libakonadi-kabc4 4:4.5.3-0ubuntu1~lucid1~ppa1 library for using the Akonadi PIM data server
ii libakonadi-kcal4 4:4.5.3-0ubuntu1~lucid1~ppa1 library for using the Akonadi PIM data server
ii libakonadi-kde4 4:4.5.3-0ubuntu1~lucid1~ppa1 library for using the Akonadi PIM data server
ii libakonadi-kmime4 4:4.5.3-0ubuntu1~lucid1~ppa1 library for using the Akonadi PIM data server
ii libakonadiprivate1 1.4.0-0ubuntu1~lucid1~ppa3 libraries for the Akonadi PIM storage service
ii libalgorithm-c3-perl 0.08-1 Perl module for merging hierarchies using the C3 algorithm
ii libamd2.2.0 1:3.4.0-1ubuntu3 approximate minimum degree ordering library for sparse matrices
ii libanthy0 9100h-0ubuntu2 input method for Japanese - runtime library
ii libao2 0.8.8-5ubuntu2 Cross Platform Audio Output Library
ii libapache2-mod-php5 5.3.2-1ubuntu4.9 server-side, HTML-embedded scripting language (Apache 2 module)

ii libapparmor-perl 2.5.1-0ubuntu0.10.04.3 AppArmor library Perl bindings
ii libapparmor1 2.5.1-0ubuntu0.10.04.3 changehat AppArmor library
ii libappconfig-perl 1.56-2 Perl module for configuration file and command line handling
ii libappindicator0 0.0.19-0ubuntu4 Application Indicators
ii libapr1 1.3.8-1build1 The Apache Portable Runtime Library
ii libaprutil1 1.3.9+dfsg-3ubuntu0.10.04.1 The Apache Portable Runtime Utility Library
ii libaprutil1-dbd-sqlite3 1.3.9+dfsg-3ubuntu0.10.04.1 The Apache Portable Runtime Utility Library - SQLite3 Driver
ii libaprutil1-ldap 1.3.9+dfsg-3ubuntu0.10.04.1 The Apache Portable Runtime Utility Library - LDAP Driver
ii libarchive1 2.8.0-2 Single library to read/write tar, cpio, pax, zip, iso9660, etc.
ii libart-2.0-2 2.3.20-2build1 Library of functions for 2D graphics - runtime files
ii libasm3-java 3.2-3ubuntu1 Java bytecode manipulation framework
ii libasound2 1.0.22-0ubuntu7 shared library for ALSA applications
ii libasound2-dev 1.0.22-0ubuntu7 shared library for ALSA applications -- development files
ii libasound2-plugins 1.0.22-0ubuntu6 ALSA library additional plugins
ii libaspell15 0.60.6-3ubuntu1 GNU Aspell spell-checker runtime library
ii libass4 0.9.9-0ubuntu1 library for SSA/ASS subtitles rendering
ii libast2 0.7-3 the Library of Assorted Spiffy Things
ii libatasmart4 0.17+git20100219-1git2 ATA S.M.A.R.T. reading and parsing library
ii libatk1.0-0 1.30.0-0ubuntu2.1 The ATK accessibility toolkit
ii libatk1.0-data 1.30.0-0ubuntu2.1 Common files for the ATK accessibility toolkit
ii libatk1.0-dev 1.30.0-0ubuntu2.1 Development files for the ATK accessibility toolkit
ii libatk1.0-doc 1.30.0-0ubuntu2.1 Documentation files for the ATK toolkit
ii libatm1 1:2.5.1-1.2 shared library for ATM (Asynchronous Transfer Mode)
ii libattica0 0.1.4-1ubuntu1~lucid1~ppa1 a Qt library that implements the Open Collaboration Services API
ii libattr1 1:2.4.44-1 Extended attribute shared library
ii libaudclient2 2.3-1ubuntu4 audacious dbus remote control library
ii libaudcore1 2.3-1ubuntu4 audacious core engine library
ii libaudid3tag2 2.3-1ubuntu4 audacious id3 tag manipulation library
ii libaudio2 1.9.2-3 Network Audio System - shared libraries
ii libaudiofile0 0.2.6-8ubuntu1 Open-source version of SGI's audiofile library
ii libavahi-client3 0.6.25-1ubuntu6.2 Avahi client library
ii libavahi-common-data 0.6.25-1ubuntu6.2 Avahi common data files
ii libavahi-common-dev 0.6.25-1ubuntu6.2 Development files for the Avahi common library
ii libavahi-common3 0.6.25-1ubuntu6.2 Avahi common library
ii libavahi-compat-libdnssd1 0.6.25-1ubuntu6.2 Avahi Apple Bonjour compatibility library
ii libavahi-core6 0.6.25-1ubuntu6.2 Avahi's embeddable mDNS/DNS-SD library
ii libavahi-glib-dev 0.6.25-1ubuntu6.2 Development headers for the Avahi glib integration library
ii libavahi-glib1 0.6.25-1ubuntu6.2 Avahi glib integration library
ii libavahi-qt3-1 0.6.25-1ubuntu6.2 Avahi Qt 3 integration library
ii libavc1394-0 0.5.3-1build4 control IEEE 1394 audio/video devices
ii libavcodec-extra-52 4:0.5.1-1ubuntu1.1 ffmpeg codec library
ii libavdevice52 4:0.5.1-1ubuntu1.1 ffmpeg device handling library
ii libavfilter0 4:0.5.1-1ubuntu1.1 ffmpeg video filtering library
ii libavformat52 4:0.5.1-1ubuntu1.1 ffmpeg file format library

ii libavidemux0 1:2.5.2-0ubuntu3 a free video editor - shared libraries
ii libavutil-extra-49 4:0.5.1-1ubuntu1.1 ffmpeg utility library
ii libbabl-0.0-0 0.0.22-1build1 Dynamic, any to any, pixel format conversion library
ii libbeagle1 0.3.9-1build1 library for accessing beagle using C
ii libbfb0 0.23-1 bfb protocol library
ii libbind9-60 1:9.7.0.dfsg.P1-1ubuntu0.1 BIND9 Shared Library used by BIND
ii libbinio1ldbl 1.4-14 Binary I/O stream class library
ii libbit-vector-perl 7.1-1 Perl module for bit vectors and more
ii libblas3gf 1.2-2build1 Basic Linear Algebra Subroutines 3, shared library
ii libblkid1 2.17.2-0ubuntu1.10.04.2 block device id library
ii libbluetooth3 4.60-0ubuntu8 Library to use the BlueZ Linux Bluetooth stack
ii libbogl-dev 0.1.18-3ubuntu4 Ben's Own Graphics Library - development files
ii libbogl0 0.1.18-3ubuntu4 Ben's Own Graphics Library - shared library
ii libbonobo2-0 2.24.3-0ubuntu1 Bonobo CORBA interfaces library
ii libbonobo2-common 2.24.3-0ubuntu1 Bonobo CORBA interfaces library -- support files
ii libbonoboui2-0 2.24.3-0ubuntu1 The Bonobo UI library
ii libbonoboui2-common 2.24.3-0ubuntu1 The Bonobo UI library -- common files
ii libboost-filesystem1.40.0 1.40.0-4ubuntu4 filesystem operations (portable paths, iteration over directories, etc) in C++
ii libboost-program-options1.40.0 1.40.0-4ubuntu4 program options library for C++
ii libboost-python1.40.0 1.40.0-4ubuntu4 Boost.Python Library
ii libboost-regex1.40.0 1.40.0-4ubuntu4 regular expression library for C++
ii libboost-system1.40.0 1.40.0-4ubuntu4 Operating system (e.g. diagnostics support) library
ii libboost-thread1.40.0 1.40.0-4ubuntu4 portable C++ multi-threading
ii libbrasero-media0 2.30.2-0ubuntu1.1 CD/DVD burning library for GNOME - runtime
ii libbsd0 0.2.0-1 utility functions from BSD systems - shared library
ii libburn4 0.7.6.pl00-2 library to provide CD/DVD writing functions
ii libbz2-1.0 1.0.5-4ubuntu0.1 high-quality block-sorting file compressor library - runtime
ii libc-ares2 1.7.0-1 library for asyncronous name resolves
ii libc-bin 2.11.1-0ubuntu7.8 Embedded GNU C Library: Binaries
ii libc-dev-bin 2.11.1-0ubuntu7.8 Embedded GNU C Library: Development binaries
ii libc6 2.11.1-0ubuntu7.8 Embedded GNU C Library: Shared libraries
ii libc6-dev 2.11.1-0ubuntu7.8 Embedded GNU C Library: Development Libraries and Header Files
ii libc6-i686 2.11.1-0ubuntu7.8 GNU C Library: Shared libraries [i686 optimized]
ii libcaca0 0.99.beta16-3 colour ASCII art library
ii libcairo-perl 1.061-1build1 Perl interface to the Cairo graphics library
ii libcairo2 1.8.10-2ubuntu1 The Cairo 2D vector graphics library
ii libcairo2-dev 1.8.10-2ubuntu1 Development files for the Cairo 2D graphics library
ii libcairo2-doc 1.8.10-2ubuntu1 Documentation for the Cairo Multi-platform 2D graphics library
ii libcairomm-1.0-1 1.8.4-0ubuntu1 C++ wrappers for Cairo (shared libraries)
ii libcanberra-gtk-module 0.22-1ubuntu2 translates Gtk+ widgets signals to event sounds
ii libcanberra-gtk0 0.22-1ubuntu2 Gtk+ helper for playing widget event sounds with libcanberra
ii libcanberra0 0.22-1ubuntu2 a simple abstract interface for playing event sounds
ii libcap-ng0 0.6.2-4 An alternate posix capabilities library

ii libcap2 1:2.17-2ubuntu1 support for getting/setting POSIX.1e capabilities
ii libcap2-bin 1:2.17-2ubuntu1 basic utility programs for using capabilities
ii libcarp-clan-perl 6.02-1 Perl enhancement to Carp error logging facilities
ii libccid 1.3.11-1 PC/SC driver for USB CCID smart card readers
ii libcddb2 1.3.2-0ubuntu1 library to access CDDB data - runtime files
ii libcdio-cdda0 0.81-4 library to read and control digital audio CDs
ii libcdio-paranoia0 0.81-4 library to read digital audio CDs with error correction
ii libcdio10 0.81-4 library to read and control CD-ROM
ii libcdparanoia0 3.10.2+debian-9 audio extraction tool for sampling CDs (library)
ii libchm-bin 2:0.40-2 library for dealing with Microsoft CHM files (test programs)
ii libchm1 2:0.40-2 library for dealing with Microsoft CHM files
ii libck-connector0 0.4.1-3ubuntu2 ConsoleKit libraries
ii libclamav6 0.97.3+dfsg-1ubuntu1~lucid1~ppa1 anti-virus utility for Unix - library
ii libclass-accessor-perl 0.34-1 Perl module that automatically generates accessors
ii libclass-base-perl 0.03-4 useful base class for deriving other modules
ii libclass-c3-perl 0.21-1 A pragma to use the C3 method resolution order algortihm
ii libclass-c3-xs-perl 0.13-1 Perl module to accelerate Class::C3
ii libclass-data-inheritable-perl 0.08-1 Inheritable, overridable class data
ii libclass-inspector-perl 1.24-1 Perl module that provides information about classes
ii libclass-makemethods-perl 1.01-4 Perl module for generating common types of methods
ii libclass-mop-perl 0.98-1 Perl module implementing a Meta Object Protocol (MOP)
ii libcln6 1.3.1-2 Class Library for Numbers (C++)
ii libclucene0ldbl 0.9.21b-2 library for full-featured text search engine (runtime)
ii libcolamd2.7.1 1:3.4.0-1ubuntu3 column approximate minimum degree ordering library for sparse matrices
ii libcomerr2 1.41.11-1ubuntu2.1 common error description library
ii libcommons-beanutils-java 1.8.2-1 utility for manipulating JavaBeans
ii libcommons-codec-java 1.4-2 encoder and decoders such as Base64 and hexadecimal codec
ii libcommons-collections3-java 3.2.1-4 A set of abstract data type interfaces and implementations
ii libcommons-compress-java 1.0-1 Java API for working with tar, zip and bzip2 files
ii libcommons-digester-java 1.8.1-2 Rule based XML Java object mapping tool
ii libcommons-el-java 1.0-5 Implementation of the JSP2.0 Expression Language interpreter
ii libcommons-httpclient-java 3.1-9 A Java(TM) library for creating HTTP clients
ii libcommons-logging-java 1.1.1-7 commmon wrapper interface for several logging APIs
ii libcompizconfig0 0.8.4-0ubuntu2 Settings library for plugins - OpenCompositing Project
ii libcroco3 0.6.2-1 a generic Cascading Style Sheet (CSS) parsing and manipulation toolkit
ii libcue1 1.3.0-1 CUE Sheet Parser Library
ii libcups2 1.4.3-1ubuntu1.4 Common UNIX Printing System(tm) - Core library
ii libcupscgi1 1.4.3-1ubuntu1.4 Common UNIX Printing System(tm) - CGI library
ii libcupsdriver1 1.4.3-1ubuntu1.4 Common UNIX Printing System(tm) - Driver library
ii libcupsimage2 1.4.3-1ubuntu1.4 Common UNIX Printing System(tm) - Raster image library
ii libcupsmime1 1.4.3-1ubuntu1.4 Common UNIX Printing System(tm) - MIME library
ii libcupsppdc1 1.4.3-1ubuntu1.4 Common UNIX Printing System(tm) - PPD manipulation library
ii libcurl3 7.19.7-1ubuntu1 Multi-protocol file transfer library (OpenSSL)
ii libcurl3-gnutls 7.19.7-1ubuntu1 Multi-protocol file transfer library (GnuTLS)

ii libcurl4-gnutls-dev 7.19.7-1ubuntu1 Development files and documentation for libcurl (GnuTLS)
ii libcv4 2.0.0-3ubuntu2 computer vision library
ii libcvaux4 2.0.0-3ubuntu2 computer vision extension library
ii libcwidget3 0.5.13-1ubuntu1 high-level terminal interface library for C++ (runtime files)
ii libdaemon0 0.14-2 lightweight C library for daemons - runtime library
ii libdata-dump-perl 1.15-1 Perl module to help dump data structures
ii libdata-optlist-perl 0.104-1 Parse and validate simple name/value option pairs
ii libdate-calc-perl 6.0-1 Perl library for accessing dates
ii libdate-manip-perl 6.05-1 module for manipulating dates
ii libdatrie1 0.2.2-3 Double-array trie library
ii libdb-je-java 3.3.62-3 Oracle Berkeley Database Java Edition
ii libdb4.6 4.6.21-16 Berkeley v4.6 Database Libraries [runtime]
ii libdb4.7 4.7.25-9 Berkeley v4.7 Database Libraries [runtime]
ii libdb4.7-java 4.7.25-9 Berkeley v4.7 Database Libraries for Java
ii libdb4.7-java-gcj 4.7.25-9 Berkeley v4.7 Database Libraries for Java (native code)
ii libdb4.8 4.8.24-1ubuntu1 Berkeley v4.8 Database Libraries [runtime]
ii libdbd-mysql-perl 4.012-1ubuntu1 A Perl5 database interface to the MySQL database
ii libdbd-sqlite3-perl 1.29-1 Perl DBI driver with a self-contained RDBMS
ii libdbi-perl 1.609-1build1 Perl Database Interface (DBI)
ii libdbus-1-3 1.2.16-2ubuntu4.2 simple interprocess messaging system
ii libdbus-1-dev 1.2.16-2ubuntu4.2 simple interprocess messaging system (development headers)
ii libdbus-glib-1-2 0.84-1 simple interprocess messaging system (GLib-based shared library)
ii libdbus-glib-1-dev 0.84-1 simple interprocess messaging system (GLib interface)
ii libdbusmenu-glib1 0.2.9-0ubuntu3.1 Menus over DBus shared library for glib
ii libdbusmenu-gtk1 0.2.9-0ubuntu3.1 Menus over DBus shared library for GTK
ii libdbusmenu-qt2 0.6.4-0ubuntu1~lucid1~ppa1 a Qt library that implements the DBusMenu spec
ii libdc1394-22 2.1.2-2 high level programming interface for IEEE1394 digital camera
ii libdca0 0.0.5-3 decoding library for DTS Coherent Acoustics streams
ii libdebconfclient0 0.147 Debian Configuration Management System (C-implementation)
ii libdebian-installer4 0.68ubuntu3 Library of common debian-installer functions
ii libdecoration0 1:0.8.4-0ubuntu15.3 Compiz window decoration library
ii libdevel-globaldestruction-perl 0.02-1 Expose PL_dirty, the flag which marks global destruction
ii libdevhelp-1-1 2.30.0-0ubuntu1 Library providing documentation browser functionality
ii libdevmapper1.02.1 2:1.02.39-1ubuntu4.1 The Linux Kernel Device Mapper userspace library
ii libdigest-hmac-perl 1.01-7 create standard message integrity checks
ii libdigest-sha1-perl 2.12-1build1 NIST SHA-1 message digest algorithm
ii libdirac-encoder0 1.0.2-2 open and royalty free high quality codec - encoder library
ii libdirectfb-1.2-0 1.2.8-5ubuntu2 direct frame buffer graphics - shared libraries
ii libdirectfb-dev 1.2.8-5ubuntu2 direct frame buffer graphics library - development files
ii libdirectfb-extra 1.2.8-5ubuntu2 direct frame buffer graphics - extra providers
ii libdiscover2 2.1.2-3 hardware identification library
ii libdjvulibre-text 3.5.22-1ubuntu4.1 Linguistic support files for libdjvulibre
ii libdjvulibre21 3.5.22-1ubuntu4.1 Runtime support for the DjVu image format

ii libdmraid1.0.0.rc16 1.0.0.rc16-3ubuntu2 Device-Mapper Software RAID support tool - shared library
ii libdnet 2.49ubuntu1 DECnet Libraries
ii libdnet-dev 2.49ubuntu1 DECnet development libraries & Headers
ii libdns64 1:9.7.0.dfsg.P1-1ubuntu0.1 DNS Shared Library used by BIND
ii libdrm-intel1 2.4.18-1ubuntu3 Userspace interface to intel-specific kernel DRM services -- runtime
ii libdrm-nouveau1 2.4.18-1ubuntu3 Userspace interface to nouveau-specific kernel DRM services -- runtime
ii libdrm-radeon1 2.4.18-1ubuntu3 Userspace interface to radeon-specific kernel DRM services -- runtime
ii libdrm2 2.4.18-1ubuntu3 Userspace interface to kernel DRM services -- runtime
ii libdumbnet-dev 1.12-3 A dumb, portable networking library -- development files
ii libdumbnet1 1.12-3 A dumb, portable networking library -- shared library
ii libdv4 1.0.0-2ubuntu2 software library for DV format digital video (runtime lib)
ii libdvbpsi5 0.1.6-1 library for MPEG TS and DVB PSI tables decoding and generating
ii libdvdnav4 4.1.3-6 DVD navigation library
ii libdvdread4 4.1.3-8ubuntu1 library for reading DVDs
ii libebml0 0.7.7-3.1 access library for the EBML format
ii libecj-java 3.5.1-1 Eclipse Java compiler (library)
ii libecryptfs0 83-0ubuntu3.1 ecryptfs cryptographic filesystem (library)
ii libedit2 2.11-20080614-1build1 BSD editline and history libraries
ii libeggdbus-1-0 0.6-1 D-Bus bindings for GObject
ii libelf1 0.143-1 library to read and write ELF files
ii libenca0 1.12-1 Extremely Naive Charset Analyser - shared library files
ii libenchant-dev 1.6.0-0ubuntu1 a wrapper library for various spell checker engines (development)
ii libenchant1c2a 1.6.0-0ubuntu1 a wrapper library for various spell checker engines
ii libept0 0.5.30 High-level library for managing Debian package information
ii libequinox-osgi-java 3.5.2-2ubuntu4.3 Equinox OSGi framework
ii liberror-perl 0.17-1 Perl module for error/exception handling in an OO-ish way
ii libesd0 0.2.41-6ubuntu1 Enlightened Sound Daemon - Shared libraries
ii libestools1.2 1:1.2.96~beta-6 Edinburgh Speech Tools Library
ii libetpan13 0.58-1 mail handling library
ii libevdocument2 2.30.3-0ubuntu1.2 GNOME document viewer backend library
ii libevent-1.4-2 1.4.13-stable-1 An asynchronous event notification library
ii libevent-core-1.4-2 1.4.13-stable-1 An asynchronous event notification library (core)
ii libevent-dev 1.4.13-stable-1 Development libraries, header files and docs for libevent
ii libevent-extra-1.4-2 1.4.13-stable-1 An asynchronous event notification library (extra)
ii libevview2 2.30.3-0ubuntu1.2 GNOME document viewer view library
ii libewf1 20100119-1 library with support for Expert Witness Compression Format
ii libexif12 0.6.19-1 library to parse EXIF files
ii libexiv2-6 0.19-1 EXIF/IPTC metadata manipulation library
ii libexo-0.3-0 0.3.106-1ubuntu2.1 Library with extensions for Xfce
ii libexo-common 0.3.106-1ubuntu2.1 libexo common files
ii libexpat1 2.0.1-7ubuntu1 XML parsing C library - runtime library
ii libexpat1-dev 2.0.1-7ubuntu1 XML parsing C library - development kit
ii libextractor-plugins 0.5.23+dfsg-4build1 extracts meta-data from files of arbitrary type

(plugins)
ii libextractor1c2a 0.5.23+dfsg-4build1 extracts meta-data from files of arbitrary type (library)
ii libfaac0 1.26-0.1ubuntu2 an AAC audio encoder - library files
ii libfaad2 2.7-4 freeware Advanced Audio Decoder - runtime files
ii libfbclient2 2.1.3.18185-0.ds1-6build1 Firebird client library
ii libffi5 3.0.9-1 Foreign Function Interface library runtime
ii libfftw3-3 3.2.2-1 library for computing Fast Fourier Transforms
ii libfile-copy-recursive-perl 0.38-1 Perl extension for recursively copying files and directories
ii libfile-find-rule-perl 0.32-1 module to search for files based on rules
ii libfile-homedir-perl 0.86-1 Get the home directory for yourself or other users in Perl
ii libfile-sharedir-perl 1.00-0.1 Locate per-dist and per-module shared files
ii libfile-spec-perl 3.3100-1 collection of tools for working with paths across platforms
ii libfile-which-perl 1.08-1 Perl module for searching paths for executable programs
ii libflac++6 1.2.1-2build2 Free Lossless Audio Codec - C++ runtime library
ii libflac8 1.2.1-2build2 Free Lossless Audio Codec - runtime C library
ii libfltk1.1 1.1.10-2 Fast Light Toolkit - shared libraries
ii libfluidsynth1 1.1.1-2build1 Real-time MIDI software synthesizer (runtime library)
ii libfont-afm-perl 1.20-1 Font::AFM - Interface to Adobe Font Metrics files
ii libfontconfig1 2.8.0-2ubuntu1 generic font configuration library - runtime
ii libfontconfig1-dev 2.8.0-2ubuntu1 generic font configuration library - development
ii libfontenc1 1:1.0.5-1 X11 font encoding library
ii libfreeimage3 3.10.0-2 Support library for graphics image formats (library)
ii libfreetype6 2.3.11-1ubuntu2.4 FreeType 2 font engine, shared library files
ii libfreetype6-dev 2.3.11-1ubuntu2.4 FreeType 2 font engine, development files
ii libfreezethaw-perl 0.45-1 converting Perl structures to strings and back
ii libfribidi0 0.19.2-1 Free Implementation of the Unicode BiDi algorithm
ii libfs6 2:1.0.2-1build1 X11 Font Services library
ii libfuse2 2.8.1-1.1ubuntu3.1 Filesystem in USErspace library
ii libgadu3 1:1.9.0~rc2-1 Gadu-Gadu protocol library - runtime files
ii libgail-common 2.20.1-0ubuntu2 GNOME Accessibility Implementation Library -- common modules
ii libgail18 2.20.1-0ubuntu2 GNOME Accessibility Implementation Library -- shared libraries
ii libgamin0 0.1.10-1ubuntu3 Client library for the gamin file and directory monitoring system
ii libgavl1 1.1.1-3 low level audio and video library - runtime files
ii libgc1c2 1:6.8-1.2ubuntu1 conservative garbage collector for C and C++
ii libgcc1 1:4.4.3-4ubuntu5 GCC support library
ii libgcj-bc 4.4.3-4ubuntu1 Link time only library for use with gcj
ii libgcj-common 1:4.4.3-1ubuntu1 Java runtime library (common files)
ii libgcj10 4.4.3-1ubuntu4.1 Java runtime library for use with gcj
ii libgconf2-4 2.28.1-0ubuntu1 GNOME configuration database system (shared libraries)
ii libgcr0 2.92.92.is.2.30.3-0ubuntu1.1 Library for Crypto UI related task - runtime
ii libgcrypt11 1.4.4-5ubuntu2 LGPL Crypto library - runtime library
ii libgcrypt11-dev 1.4.4-5ubuntu2 LGPL Crypto library - development files
ii libgd-gd2-noxpm-perl 1:2.39-2 Perl module wrapper for libgd - gd2 variant without XPM support

ii libgd2-xpm 2.0.36~rc1~dfsg-3.1ubuntu1 GD Graphics Library version 2
ii libgdbm3 1.8.3-9 GNU dbm database routines (runtime version)
ii libgdu0 2.30.1-1 GObject based Disk Utility Library
ii libgegl-0.0-0 0.0.22-0ubuntu4 Generic Graphics Library
ii libgeoip1 1.4.6.dfsg-17 A non-DNS IP-to-country resolver library
ii libgfortran3 4.4.3-4ubuntu5 Runtime library for GNU Fortran applications
ii libgif-dev 4.1.6-9 library for GIF images (development)
ii libgif4 4.1.6-9 library for GIF images (library)
ii libgimp2.0 2.6.8-2ubuntu1.2 Libraries for the GNU Image Manipulation Program
ii libgksu2-0 2.0.13~pre1-1ubuntu4.1 library providing su and sudo functionality
ii libgl1-mesa-dri 7.7.1-1ubuntu3 A free implementation of the OpenGL API -- DRI modules
ii libgl1-mesa-glx 7.7.1-1ubuntu3 A free implementation of the OpenGL API -- GLX runtime
ii libglade2-0 1:2.6.4-1build1 library to load .glade files at runtime
ii libglib-perl 1:1.222-1 Perl interface to the GLib and GObject libraries
ii libglib2.0-0 2.24.1-0ubuntu1 The GLib library of C routines
ii libglib2.0-dev 2.24.1-0ubuntu1 Development files for the GLib library
ii libglib2.0-doc 2.24.1-0ubuntu1 Documentation files for the GLib library
ii libglibmm-2.4-1c2a 2.24.2-0ubuntu1 C++ wrapper for the GLib toolkit (shared libraries)
ii libglu1-mesa 7.7.1-1ubuntu3 The OpenGL utility library (GLU)
ii libgmime-2.4-2 2.4.14-1+nmu1 MIME message parser and creator library - runtime
ii libgmp3c2 2:4.3.2+dfsg-1ubuntu1 Multiprecision arithmetic library
ii libgnome-desktop-2-17 1:2.30.2-0ubuntu1 Utility library for loading .desktop files - runtime files
ii libgnome-keyring0 2.30.1-0ubuntu1 GNOME keyring services library
ii libgnome-menu2 2.30.0-0ubuntu4 an implementation of the freedesktop menu specification for GNOME
ii libgnome-window-settings1 1:2.30.1-0ubuntu1 Utility library for getting window manager settings
ii libgnome2-0 2.30.0-0ubuntu1 The GNOME library - runtime files
ii libgnome2-canvas-perl 1.002-2build1 Perl interface to the GNOME canvas library
ii libgnome2-common 2.30.0-0ubuntu1 The GNOME library - common files
ii libgnome2-perl 1.042-2build1 Perl interface to the GNOME libraries
ii libgnome2-vfs-perl 1.081-1build1 Perl interface to the 2.x series of the GNOME VFS library
ii libgnomecanvas2-0 2.30.1-0ubuntu1 A powerful object-oriented display - runtime files
ii libgnomecanvas2-common 2.30.1-0ubuntu1 A powerful object-oriented display - common files
ii libgnomecups1.0-1 0.2.3-3build2 GNOME library for CUPS interaction
ii libgnomeprint2.2-0 2.18.6-1build2 The GNOME 2.2 print architecture - runtime files
ii libgnomeprint2.2-data 2.18.6-1build2 The GNOME 2.2 print architecture - data files
ii libgnomeprintui2.2-0 2.18.4-1build1 GNOME 2.2 print architecture User Interface - runtime files
ii libgnomeprintui2.2-common 2.18.4-1build1 GNOME 2.2 print architecture User Interface - common files
ii libgnomeui-0 2.24.3-1 The GNOME libraries (User Interface) - runtime files
ii libgnomeui-common 2.24.3-1 The GNOME libraries (User Interface) - common files
ii libgnomevfs2-0 1:2.24.2-1ubuntu2 GNOME Virtual File System (runtime libraries)
ii libgnomevfs2-common 1:2.24.2-1ubuntu2 GNOME Virtual File System (common files)

ii libgnomevfs2-extra 1:2.24.2-1ubuntu2 GNOME Virtual File System (extra modules)
ii libgnutls-dev 2.8.5-2 the GNU TLS library - development files
ii libgnutls26 2.8.5-2 the GNU TLS library - runtime library
ii libgomp1 4.4.3-4ubuntu5 GCC OpenMP (GOMP) support library
ii libgoocanvas-common 0.15-0ubuntu2 new canvas widget for GTK+ that uses the cairo 2D library
ii libgoocanvas3 0.15-0ubuntu2 new canvas widget for GTK+ that uses the cairo 2D library
ii libgp11-0 2.92.92.is.2.30.3-0ubuntu1.1 Glib wrapper library for PKCS#11 - runtime
ii libgpg-error-dev 1.6-1ubuntu2 library for common error values and messages in GnuPG components
ii libgpg-error0 1.6-1ubuntu2 library for common error values and messages in GnuPG components
ii libgpgme++2 4:4.5.3-0ubuntu1~lucid1~ppa1 c++ wrapper library for gpgme
ii libgpgme11 1.2.0-1.2ubuntu1 GPGME - GnuPG Made Easy
ii libgphoto2-2 2.4.8-0ubuntu2 gphoto2 digital camera library
ii libgphoto2-port0 2.4.8-0ubuntu2 gphoto2 digital camera port library
ii libgpm2 1.20.4-3.2ubuntu2 General Purpose Mouse - shared library
ii libgps19 2.92-4 Global Positioning System - library
ii libgraph-perl 1:0.91-1 Perl module for graph data structures and algorithms
ii libgraphite3 1:2.3.1-0.2 SILGraphite - a "smart font" rendering engine
ii libgraphviz-perl 2.04-1 Perl interface to the GraphViz graphing tool
ii libgraphviz4 2.20.2-8ubuntu3 rich set of graph drawing tools
ii libgs8 8.71.dfsg.1-0ubuntu5.3 The Ghostscript PostScript/PDF interpreter Library
ii libgsf-1-114 1.14.16-1ubuntu1 Structured File Library - runtime version
ii libgsf-1-common 1.14.16-1ubuntu1 Structured File Library - common files
ii libgsl0ldbl 1.13+dfsg-1 GNU Scientific Library (GSL) -- library package
ii libgsm1 1.0.13-3 Shared libraries for GSM speech compressor
ii libgsm1-dev 1.0.13-3 Development libraries for a GSM speech compressor
ii libgssapi-krb5-2 1.8.1+dfsg-2ubuntu0.9 MIT Kerberos runtime libraries - krb5 GSS-API Mechanism
ii libgssdp-1.0-2 0.7.1-1 GObject-based library for SSDP
ii libgssglue1 0.1-4 mechanism-switch gssapi library
ii libgssrpc4 1.8.1+dfsg-2ubuntu0.9 MIT Kerberos runtime libraries - GSS enabled ONCRPC
ii libgstfarsight0.10-0 0.0.17-2ubuntu2 Audio/Video communications framework: core library
ii libgstreamer-plugins-base0.10-0 0.10.28-1 GStreamer libraries from the "base" set
ii libgstreamer0.10-0 0.10.28-1 Core GStreamer libraries and elements
ii libgstreamer0.10-dev 0.10.28-1 GStreamer core development files
ii libgtk2-perl 1:1.221-4ubuntu2 Perl interface to the 2.x series of the Gimp Toolkit library
ii libgtk2.0-0 2.20.1-0ubuntu2 The GTK+ graphical user interface library
ii libgtk2.0-bin 2.20.1-0ubuntu2 The programs for the GTK+ graphical user interface library
ii libgtk2.0-common 2.20.1-0ubuntu2 Common files for the GTK+ graphical user interface library
ii libgtk2.0-dev 2.20.1-0ubuntu2 Development files for the GTK+ library
ii libgtk2.0-doc 2.20.1-0ubuntu2 Documentation for the GTK+ graphical user interface library
ii libgtkglext1 1.2.0-1ubuntu1 OpenGL Extension to GTK+ (shared libraries)
ii libgtkhex0 2.24.0-1 GNOME Hex editor for files (shared library)

ii libgtkimageview0 1.6.1-2 image viewer widget for GTK+
ii libgtkmm-2.4-1c2a 1:2.20.3-0ubuntu1 C++ wrappers for GTK+ (shared libraries)
ii libgtksourceview2.0-0 2.10.4-0ubuntu1 shared libraries for the GTK+ syntax highlighting widget
ii libgtksourceview2.0-common 2.10.4-0ubuntu1 common files for the GTK+ syntax highlighting widget
ii libgtkspell-dev 2.0.16-1 Development files for GtkSpell
ii libgtkspell0 2.0.16-1 a spell-checking addon for GTK's TextView widget
ii libgtop2-7 2.26.1-0ubuntu2 gtop system monitoring library
ii libgtop2-common 2.26.1-0ubuntu2 common files for the gtop system monitoring library
ii libgudev-1.0-0 1:151-12.3 GObject-based wrapper library for libudev
ii libgupnp-1.0-3 0.13.2-1ubuntu1 GObject-based library for UPnP
ii libgupnp-igd-1.0-2 0.1.3-4ubuntu1 library to handle UPnP IGD port mapping
ii libgutenprint2 5.2.5-0ubuntu1.1 runtime for the Gutenprint printer driver library
ii libgvfscommon0 1.6.1-0ubuntu1build1 userspace virtual filesystem - library
ii libhal-storage1 0.5.14-0ubuntu6 Hardware Abstraction Layer - shared library for storage devices
ii libhal1 0.5.14-0ubuntu6 Hardware Abstraction Layer - shared library
ii libhamcrest-java 1.1-4 library of matchers for building test expressions
ii libheap-perl 0.80-2 Perl extensions for keeping data partially sorted
ii libhighgui4 2.0.0-3ubuntu2 computer vision GUI library
ii libhijack 0.5.2-bt0 Runtime Process Infection Made Easy
ii libhpmud0 3.10.2-2ubuntu2.2 HP Multi-Point Transport Driver (hpmud) run-time libraries
ii libhsqldb-java 1.8.0.10-6ubuntu2 Java SQL database engine
ii libhtml-format-perl 2.04-2 format HTML syntax trees into text, PostScript or RTF
ii libhtml-parser-perl 3.64-1 collection of modules that parse HTML text documents
ii libhtml-tagset-perl 3.20-2 Data tables pertaining to HTML
ii libhtml-template-perl 2.9-1 HTML::Template : A module for using HTML Templates with Perl
ii libhtml-tree-perl 3.23-1 represent and create HTML syntax trees
ii libhttp-dav-perl 0.38-1 WebDAV client library for Perl, and "dave" CLI client
ii libhttp-server-simple-perl 0.41-1 simple stand-alone HTTP server
ii libhttrack2 3.43.9-1ubuntu1 Httrack website copier library
ii libhunspell-1.2-0 1.2.8-6ubuntu1 spell checker and morphological analyzer (shared library)
ii libhyphen0 2.4-6ubuntu1 ALTLinux hyphenation library - shared library
ii libiaxclient-dev 2.0.2-3build1 Portable IAX(2) protocol telephony client - development files
ii libiaxclient1 2.0.2-3build1 Portable IAX(2) protocol telephony client - shared library
ii libibus1 1.2.0.20091215-1ubuntu4 New input method framework using dbus
ii libical0 0.44-3 iCalendar library implementation in C (runtime)
ii libice-dev 2:1.0.6-1 X11 Inter-Client Exchange library (development headers)
ii libice6 2:1.0.6-1 X11 Inter-Client Exchange library
ii libicu42 4.2.1-3 International Components for Unicode
ii libicu4j-java 4.0.1.1-1 Library for unicode support and internalisation
ii libid3-3.8.3c2a 3.8.3-7.2ubuntu4 Library for manipulating ID3v1 and ID3v2 tags.
ii libid3tag0 0.15.1b-10build2 ID3 tag reading library from the MAD project
ii libidl0 0.8.13-1 library for parsing CORBA IDL files

ii libidn11 1.15-2 GNU Libidn library, implementation of IETF IDN specifications
ii libidn11-dev 1.15-2 Development files for GNU Libidn, an IDN library
ii libido-0.1-0 0.1.6-0ubuntu1 Shared library providing extra gtk menu items for display in
ii libiec61883-0 1.2.0-0.1build1 an partial implementation of IEC 61883
ii libijs-0.35 0.35-7build1 IJS raster image transport protocol: shared library
ii libilmbase6 1.0.1-3build2 several utility libraries from ILM used by OpenEXR
ii libimage-exiftool-perl 7.89-1 Library and program to read and write meta information in multimedia files
ii libimlib2 1.4.2-5build1 powerful image loading and rendering library
ii libimobiledevice0 0.9.7-1ubuntu1 Library for communicating with the iPhone and iPod Touch
ii libindicate-gtk2 0.3.6-0ubuntu1 GNOME panel indicator applet - shared library
ii libindicate4 0.3.6-0ubuntu1 GNOME panel indicator applet - shared library
ii libindicator0 0.3.8-0ubuntu1 GNOME panel indicator applet - shared library
ii libio-pty-perl 1:1.07-2build1 Perl module for pseudo tty IO
ii libio-socket-ssl-perl 1.31-1 Perl module implementing object oriented interface to SSL sockets
ii libio-string-perl 1.08-2 Emulate IO::File interface for in-core strings
ii libio-stringy-perl 2.110-4 Perl modules for IO from scalars and arrays
ii libiodbc2 3.52.6-4 iODBC Driver Manager
ii libipc-run-perl 0.84-1 Perl module for running processes
ii libisc60 1:9.7.0.dfsg.P1-1ubuntu0.1 ISC Shared Library used by BIND
ii libiscсc60 1:9.7.0.dfsg.P1-1ubuntu0.1 Command Channel Library used by BIND
ii libisccfg60 1:9.7.0.dfsg.P1-1ubuntu0.1 Config File Handling Library used by BIND
ii libiso9660-7 0.81-4 library to work with ISO9660 filesystems
ii libisofs6 0.6.26-2 library to create ISO9960 images
ii libiw30 30~pre9-3ubuntu4 Wireless tools - library
ii libjack0 0.118+svn3796-1ubuntu2 JACK Audio Connection Kit (libraries)
ii libjasper-java 5.5.26-5 Implementation of the JSP Container
ii libjasper1 1.900.1-7 The JasPer JPEG-2000 runtime library
ii libjaxp1.3-java 1.3.04-5ubuntu3 Java XML parser and transformer APIs (DOM, SAX, JAXP, TrAX)
ii libjcode-pm-perl 2.06-1 Perl extension interface to convert Japanese text
ii libjetty-java 6.1.22-1ubuntu1 Java servlet engine and webserver -- core libraries
ii libjline-java 0.9.94-5 Java library for handling console input
ii libjpeg-progs 7+really6b-15ubuntu1 Programs for manipulating JPEG files
ii libjpeg62 6b-15ubuntu1 The Independent JPEG Group's JPEG runtime library
ii libjpeg62-dev 6b-15ubuntu1 Development files for the IJG JPEG library
ii libjs-jquery 1.3.3-2ubuntu1 JavaScript library for dynamic web applications
ii libjs-mootools 1.2.4.0~debian1-1 compact JavaScript framework
ii libjsch-java 0.1.42-1ubuntu0.1 pure Java implementation of the SSH2 protocol
ii libjson-glib-1.0-0 0.7.6-0ubuntu2 GLib JSON manipulation library
ii libjtidy-java 7+svn20070309-4 a Java port of HTML Tidy, a HTML syntax checker and pretty printer
ii libjudydebian1 1.0.5-1 C library for creating and accessing dynamic arrays
ii libk3b6 2.0.1-1ubuntu3~lucid1~ppa1 The KDE CD/DVD burning application library - runtime files
ii libk5crypto3 1.8.1+dfsg-2ubuntu0.9 MIT Kerberos runtime libraries - Crypto Library

ii libkabc4 4:4.5.3-0ubuntu1~lucid1~ppa1 library for handling address book data
ii libkadm5clnt-mit7 1.8.1+dfsg-2ubuntu0.9 MIT Kerberos runtime libraries - Administration Clients
ii libkadm5srv-mit7 1.8.1+dfsg-2ubuntu0.9 MIT Kerberos runtime libraries - KDC and Admin Server
ii libkatepartinterfaces4 4:4.5.3-0ubuntu1~lucid1~ppa2 Kate part library
ii libkblog4 4:4.5.3-0ubuntu1~lucid1~ppa1 client-side support library for web application remote blogging APIs
ii libkcal4 4:4.5.3-0ubuntu1~lucid1~ppa1 library for handling calendar data
ii libkcddb4 4:4.5.3-0ubuntu1~lucid1~ppa1 CDDB library for KDE (runtime)
ii libkdb5-4 1.8.1+dfsg-2ubuntu0.9 MIT Kerberos runtime libraries - Kerberos database
ii libkde3support4 4:4.5.3-0ubuntu1~lucid1~ppa2 the KDE 3 Support Library for the KDE 4 Platform
ii libkdecorations4 4:4.5.3-0ubuntu1~lucid1~ppa1 library used by decorations for the KDE 4 window manager
ii libkdecore5 4:4.5.3-0ubuntu1~lucid1~ppa2 the KDE Platform Core Library
ii libkdepim4 4:4.4.8-0ubuntu0.0.1 KDE PIM library
ii libkdesu5 4:4.5.3-0ubuntu1~lucid1~ppa2 the Console-mode Authentication Library for the KDE Platform
ii libkdeui5 4:4.5.3-0ubuntu1~lucid1~ppa2 the KDE Platform User Interface Library
ii libkdewebkit5 4:4.5.3-0ubuntu1~lucid1~ppa2 the KDE WebKit Library
ii libkdnssd4 4:4.5.3-0ubuntu1~lucid1~ppa2 the DNS-SD Protocol Library for the KDE Platform
ii libkephal4 4:4.5.3-0ubuntu1~lucid1~ppa1 API for easier handling of multihead systems
ii libkexiv2-8 4:4.5.3-0ubuntu1~lucid1~ppa1 Qt like interface for the libexiv2 library (runtime)
ii libkeyutils1 1.2-12 Linux Key Management Utilities (library)
ii libkfile4 4:4.5.3-0ubuntu1~lucid1~ppa2 the File Selection Dialog Library for KDE Platform
ii libkholidays4 4:4.5.3-0ubuntu1~lucid1~ppa1 holidays calculation library
ii libkhtml5 4:4.5.3-0ubuntu1~lucid1~ppa2 the KHTML Web Content Rendering Engine
ii libkimap4 4:4.5.3-0ubuntu1~lucid1~ppa1 library for handling IMAP data
ii libkimproxy4 4:4.5.3-0ubuntu1~lucid1~ppa2 the Instant Messaging Interface Library for the KDE Platform
ii libkio5 4:4.5.3-0ubuntu1~lucid1~ppa2 the Network-enabled File Management Library for the KDE Platform
ii libkipi7 4:4.5.3-0ubuntu1~lucid1~ppa1 library for apps that want to use kipi-plugins (runtime version)
ii libkjsapi4 4:4.5.3-0ubuntu1~lucid1~ppa2 the KJS API Library for the KDE Development Platform
ii libkjsembed4 4:4.5.3-0ubuntu1~lucid1~ppa2 library for binding JavaScript objects to QObjects
ii libkldap4 4:4.5.3-0ubuntu1~lucid1~ppa1 library for accessing LDAP
ii libkleo4 4:4.4.8-0ubuntu0.0.1 certificate based crypto library for KDE
ii libklibc 1.5.17-4ubuntu1 minimal libc subset for use with initramfs
ii libkmediaplayer4 4:4.5.3-0ubuntu1~lucid1~ppa2 the KMediaPlayer Interface for the KDE Platform
ii libkmime4 4:4.5.3-0ubuntu1~lucid1~ppa1 library for handling MIME data
ii libknewstuff2-4 4:4.5.3-0ubuntu1~lucid1~ppa2 the "Get Hot New Stuff" v2 Library for the

KDE Platform
ii libknewstuff3-4 4:4.5.3-0ubuntu1~lucid1~ppa2 the "Get Hot New Stuff" v3 Library for the KDE Platform
ii libknotifyconfig4 4:4.5.3-0ubuntu1~lucid1~ppa2 library for configuring KDE Notifications
ii libkntlm4 4:4.5.3-0ubuntu1~lucid1~ppa2 the NTLM Authentication Library for the KDE Platform
ii libkonq5 4:4.5.3-0ubuntu1~lucid1~ppa1 core libraries for Konqueror
ii libkonq5-templates 4:4.5.3-0ubuntu1~lucid1~ppa1 data files for the Konqueror libraries
ii libkonqsidebarplugin4a 4:4.5.3-0ubuntu1~lucid1~ppa1 Konqueror sidebar plugin library
ii libkparts4 4:4.5.3-0ubuntu1~lucid1~ppa2 the Framework for the KDE Platform Graphical Components
ii libkpathsea5 2009-5ubuntu0.2 TeX Live: path search library for TeX (runtime part)
ii libkpgp4 4:4.4.8-0ubuntu0.0.1 gpg based crypto library for KDE
ii libkpimidentities4 4:4.5.3-0ubuntu1~lucid1~ppa1 library for managing user identities
ii libkpimtextedit4 4:4.5.3-0ubuntu1~lucid1~ppa1 library that provides a textedit with PIM-specific features
ii libkpimutils4 4:4.5.3-0ubuntu1~lucid1~ppa1 library for dealing with email addresses
ii libkpty4 4:4.5.3-0ubuntu1~lucid1~ppa2 the Pseudo Terminal Library for the KDE Platform
ii libkrb5-3 1.8.1+dfsg-2ubuntu0.9 MIT Kerberos runtime libraries
ii libkrb5-dev 1.8.1+dfsg-2ubuntu0.9 Headers and development libraries for MIT Kerberos
ii libkrb5support0 1.8.1+dfsg-2ubuntu0.9 MIT Kerberos runtime libraries - Support library
ii libkresources4 4:4.5.3-0ubuntu1~lucid1~ppa1 the KDE Resource framework library
ii libkrosscore4 4:4.5.3-0ubuntu1~lucid1~ppa2 the Kross Core Library
ii libkrossui4 4:4.5.3-0ubuntu1~lucid1~ppa2 the Kross UI Library
ii libksba8 1.0.7-2 X.509 and CMS support library
ii libkscreensaver5 4:4.5.3-0ubuntu1~lucid1~ppa1 library of the KDE Screensaver system
ii libksgrd4 4:4.5.3-0ubuntu1~lucid1~ppa1 library for the ksysguard GUI
ii libksignalplotter4 4:4.5.3-0ubuntu1~lucid1~ppa1 the KSignalPlotter widget
ii libktexteditor4 4:4.5.3-0ubuntu1~lucid1~ppa2 the KTextEditor interfaces for the KDE Platform
ii libktnef4 4:4.5.3-0ubuntu1~lucid1~ppa1 library for handling TNEF data
ii libktorrent-l10n 1.0.3-0ubuntu1~lucid1~ppa2 localization files for the KTorrent library
ii libktorrent2 1.0.3-0ubuntu1~lucid1~ppa2 the KTorrent library for C++ / Qt 4 / KDE Platform
ii libkunitconversion4 4:4.5.3-0ubuntu1~lucid1~ppa2 the Unit Conversion library for the KDE Platform
ii libkutils4 4:4.5.3-0ubuntu1~lucid1~ppa2 various utility classes for the KDE Platform
ii libkwineffects1a 4:4.5.3-0ubuntu1~lucid1~ppa1 library used by effects for the KDE 4 window manager
ii libkworkspace4 4:4.5.3-0ubuntu1~lucid1~ppa1 library for the kdebase workspace
ii libkxmlrpcclient4 4:4.5.3-0ubuntu1~lucid1~ppa1 simple XML-RPC client library
ii liblapack3gf 3.2.1-2 library of linear algebra routines 3 - shared version
ii liblash2 0.5.4-0ubuntu5 Linux Audio Session Handler (LASH) shared library files
ii liblaunchpad-integration1 0.1.35 library for launchpad integration
ii liblcms1 1.18.dfsg-1ubuntu2.10.04.1 Color management library
ii libldap-2.4-2 2.4.21-0ubuntu5.4 OpenLDAP libraries
ii libldap2-dev 2.4.21-0ubuntu5.4 OpenLDAP development libraries
ii liblircclient0 0.8.6-0ubuntu4.2 infra-red remote control support - client library

ii liblist-moreutils-perl 0.25~02-1 Perl module with additional list functions not found in List::Util
ii liblocale-gettext-perl 1.05-6 Using libc functions for internationalization in Perl
ii liblockfile1 1.08-3ubuntu1 NFS-safe locking library, includes dotlockfile program
ii liblog4cpp5 1.0-4 C++ library for flexible logging (runtime)
ii libltdl-dev 2.2.6b-2ubuntu1 A system independent dlopen wrapper for GNU libtool
ii libltdl7 2.2.6b-2ubuntu1 A system independent dlopen wrapper for GNU libtool
ii liblua5.1-0 5.1.4-5 Simple, extensible, embeddable programming language
ii liblua50 5.0.3-4 Main interpreter library for the Lua 5.0 programming language
ii liblualib50 5.0.3-4 Extension library for the Lua 5.0 programming language
ii liblucene2-java 2.9.2+ds1-1 Full-text search engine library for Java(TM)
ii liblwres60 1:9.7.0.dfsg.P1-1ubuntu0.1 Lightweight Resolver Library used by BIND
ii liblzma1 4.999.9beta+20091116-1 XZ-format compression library
ii liblzo2-2 2.03-2 data compression library
ii libmad0 0.15.1b-4ubuntu1 MPEG audio decoder library
ii libmagic1 5.03-5ubuntu1 File type determination library using "magic" numbers
ii libmagick++2 7:6.5.7.8-1ubuntu1.1 object-oriented C++ interface to ImageMagick
ii libmagickcore2 7:6.5.7.8-1ubuntu1.1 low-level image manipulation library
ii libmagickcore2-extra 7:6.5.7.8-1ubuntu1.1 low-level image manipulation library - extra codecs
ii libmagickwand2 7:6.5.7.8-1ubuntu1.1 image manipulation library
ii libmail-sendmail-perl 0.79.16-1 Send email from a perl script
ii libmailtools-perl 2.05-1 Manipulate email in perl programs
ii libmailtransport4 4:4.5.3-0ubuntu1~lucid1~ppa1 mail transport service library
ii libmarblewidget10 4:4.5.3-0ubuntu1~lucid1~ppa3 Marble globe widget library
ii libmatroska0 0.8.1-1.1 extensible open standard audio/video container format
ii libmcrypt4 2.5.8-3.1 De-/Encryption Library
ii libmcs1 0.7.1-1 Abstraction library to store configuration settings (BSD-licensed)
ii libmdbtools 0.5.99.0.6pre1.0.20051109-6 mdbtools libraries
ii libmeanwhile-dev 1.0.2-3build2 development package for libmeanwhile1
ii libmeanwhile1 1.0.2-3build2 open implementation of the Lotus Sametime Community Client protocol
ii libmetacity-private0 1:2.30.1-0ubuntu1.1 library for the Metacity window manager
ii libmicroblog4 4:4.5.3-0ubuntu1~lucid1~ppa1 library for using the Microblog Akonadi Resource
ii libmicrohttpd5 0.4.4-1 library embedding HTTP server functionality
ii libmjpegtools-1.9 1:1.9.0-0.5ubuntu3 MJPEG video capture/editting/playback MPEG encoding
ii libmldbm-perl 2.01-3 Store multidimensional hash structures in perl tied hashes
ii libmlt++3 0.5.4-1 MLT multimedia framework C++ wrapper (runtime)
ii libmlt-data 0.5.4-1 multimedia framework (data)
ii libmlt2 0.5.4-1 multimedia framework (runtime)
ii libmms0 0.4-2 MMS stream protocol library - shared library
ii libmng1 1.0.9-1ubuntu1 Multiple-image Network Graphics library
ii libmodplug0c2 1:0.8.7-1build1 shared libraries for mod music based on ModPlug
ii libmoose-perl 0.94-1 Modern Perl object system framework
ii libmowgli1 0.6.1-1 a high performance development framework for C
ii libmp3lame0 3.98.2+debian-0ubuntu3 An MP3 encoding library

ii libmp3splt-mp3 0.5.6-1 MP3 plugin for mp3splt
ii libmp3splt-ogg 0.5.6-1 Ogg Vorbis plugin for mp3splt
ii libmp3splt0 0.5.6-1 library for splitting MP3 and Ogg Vorbis files
ii libmpcdec3 1:1.2.2-2.1ubuntu1 Musepack (MPC) format library
ii libmpeg2-4 0.4.1-3 MPEG1 and MPEG2 video decoder library
ii libmpeg3-1 1.5.4-5 MPEG streams decoding library
ii libmpfr1ldbl 2.4.2-3ubuntu1 multiple precision floating-point computation
ii libmpg123-0 1.12.1-0ubuntu1 MPEG layer 1/2/3 audio decoder -- runtime library
ii libmro-compat-perl 0.11-1 mro::* interface compatibility for Perls < 5.9.5
ii libmtp8 1.0.2-1ubuntu1 Media Transfer Protocol (MTP) library
ii libmulticobex1 0.23-1 multi-protocol cable OBEX library
ii libmusicbrainz4c2a 2.1.5-4 Second generation incarnation of the CD Index - library
ii libmysqlclient-dev 5.1.41-3ubuntu12.10 MySQL database development files
ii libmysqlclient16 5.1.41-3ubuntu12.10 MySQL database client library
ii libnautilus-extension1 1:2.31.1-0ubuntu2~ppa92 libraries for nautilus components - runtime version
ii libncp 2.2.6-7 shared library used by programs that use NetWare Core Protocol
ii libncurses5 5.7+20090803-2ubuntu3 shared libraries for terminal handling
ii libncurses5-dev 5.7+20090803-2ubuntu3 developer's libraries and docs for ncurses
ii libncursesw5 5.7+20090803-2ubuntu3 shared libraries for terminal handling (wide character support)
ii libneon27-gnutls 0.29.0-1 An HTTP and WebDAV client library (GnuTLS enabled)
ii libnepomuk4 4:4.5.3-0ubuntu1~lucid1~ppa2 the Nepomuk Meta Data Library
ii libnepomukquery4a 4:4.5.3-0ubuntu1~lucid1~ppa2 the Nepomuk Query Library for the KDE Platform
ii libnet-daemon-perl 0.43-1 Perl module for building portable Perl daemons easily
ii libnet-dns-perl 0.65-1build1 Perform DNS queries from a Perl script
ii libnet-ip-perl 1.25-2 Perl extension for manipulating IPv4/IPv6 addresses
ii libnet-libidn-perl 0.12.ds-1 Perl bindings for GNU Libidn
ii libnet-netmask-perl 1.9015-3 parse, manipulate and lookup IP network blocks
ii libnet-pcap-perl 0.16-2 Perl binding to the LBL pcap packet capture library
ii libnet-rawip-perl 0.25-1 Perl interface to lowlevel TCP/IP
ii libnet-smtp-ssl-perl 1.01-2 SSL support for Net::SMTP
ii libnet-snmp-perl 5.2.0-3 Script SNMP connections
ii libnet-ssh-perl 0.09-1 Perl extension for secure shell
ii libnet-ssleay-perl 1.35-2ubuntu1 Perl module for Secure Sockets Layer (SSL)
ii libnet-telnet-perl 3.03-3 Script telnetable connections
ii libnet1 1.1.4-2 library for the construction and handling of network packets
ii libnet6-1.3-0 1:1.3.11-1 Network access framework for IPv4/IPv6
ii libnetpacket-perl 0.41.1-1 Modules to assemble/disassemble network packets at the protocol level
ii libnetpbm10 2:10.0-12.1ubuntu1 Graphics conversion tools shared libraries
ii libnewt0.52 0.52.10-5ubuntu1 Not Erik's Windowing Toolkit - text mode windowing with slang
ii libnfsidmap2 0.23-2 An nfs idmapping library
ii libnice0 0.0.10-2build1 ICE library (shared library)
ii libnids1.21 1.23-1.1 IP defragmentation TCP segment reassembly library
ii libnih-dbus1 1.0.1-1 NIH D-Bus Bindings Library

ii libnih1 1.0.1-1 NIH Utility Library
ii libnl1 1.1-5build1 library for dealing with netlink sockets
ii libnm-glib-dev 0.8-0ubuntu3 network management framework (GLib interface)
ii libnm-glib2 0.8-0ubuntu3 network management framework (GLib shared library)
ii libnm-util-dev 0.8-0ubuntu3 network management framework (development files)
ii libnm-util1 0.8-0ubuntu3 network management framework (shared library)
ii libnmap-parser-perl 1.05-2 parse nmap scan data with perl
ii libnotify1 0.4.5-1ubuntu4 sends desktop notifications to a notification daemon
ii libnspr4-0d 4.8.6-0ubuntu0.10.04.2 NetScape Portable Runtime Library
ii libnss-mdns 0.10-3ubuntu4 NSS module for Multicast DNS name resolution
ii libnss3-1d 3.12.9+ckbi-1.82-0ubuntu0.10.04.1 Network Security Service libraries
ii libntfs-3g75 1:2010.3.6-1ubuntu1 ntfs-3g filesystem in userspace (FUSE) library
ii libntfs10 2.0.0-1ubuntu4 library that provides common NTFS access functions
ii libnumber-compare-perl 0.01-6 module for performing numeric comparisons in Perl
ii libobexftp0 0.23-1 object exchange file transfer library
ii libogg0 1.1.4~dfsg-2 Ogg bitstream library
ii liboil0.3 0.3.16-1ubuntu2 Library of Optimized Inner Loops
ii libokularcore1 4:4.5.3-0ubuntu1~lucid1~ppa1 libraries for the Okular document viewer
ii libole-storage-lite-perl 0.19-1 simple class for OLE document interface
ii liboop4 1.0-6 Event loop management library
ii libopenal1 1:1.12.854-0ubuntu1~lucid1 Software implementation of the OpenAL API (shared library)
ii libopencore-amrnb0 0.1.2-1 Adaptive Multi Rate speech codec - shared library
ii libopencore-amrwb0 0.1.2-1 Adaptive Multi-Rate - Wideband speech codec - shared library
ii libopenexr6 1.6.1-4.1 runtime files for the OpenEXR image library
ii libopenjpeg2 1.3+dfsg-4 JPEG 2000 image compression/decompression library
ii libopenobex1 1.5-2build1 OBEX protocol library
ii libopenssl-ruby 4.2-2~uorppa0 OpenSSL interface for Ruby
ii libopenssl-ruby1.8 1.8.7.249-2 OpenSSL interface for Ruby 1.8
ii libopenssl-ruby1.9.2 1.9.2.z1-1ppa1~lucid OpenSSL interface for Ruby 1.9.2
ii libopts25 1:5.10-1.1 automated option processing library based on autogen
ii liborbit2 1:2.14.18-0.1 libraries for ORBit2 - a CORBA ORB
ii libossp-uuid16 1.6.2-1ubuntu1 OSSP uuid ISO-C and C++ - shared library
ii libotr2 3.2.0-2 Off-the-Record Messaging library
ii libpackagekit-glib2-12 0.5.7-0ubuntu2.2 Advanced library for accessing PackageKit using GLib
ii libpackagekit-qt-12 0.5.7-0ubuntu2.2 Library for accessing PackageKit using Qt.
ii libpam-ck-connector 0.4.1-3ubuntu2 ConsoleKit PAM module
ii libpam-gnome-keyring 2.92.92.is.2.30.3-0ubuntu1.1 PAM module to unlock the GNOME keyring upon login
ii libpam-modules 1.1.1-2ubuntu5.1 Pluggable Authentication Modules for PAM
ii libpam-runtime 1.1.1-2ubuntu5.1 Runtime support for the PAM library
ii libpam0g 1.1.1-2ubuntu5.1 Pluggable Authentication Modules library
ii libpango-perl 1.221-2 Perl module to layout and render international text
ii libpango1.0-0 1.28.0-0ubuntu2.2 Layout and rendering of internationalized text
ii libpango1.0-common 1.28.0-0ubuntu2.2 Modules and configuration files for the Pango
ii libpango1.0-dev 1.28.0-0ubuntu2.2 Development files for the Pango

ii libpango1.0-doc 1.28.0-0ubuntu2.2 Documentation files for the Pango
ii libpangomm-1.4-1 2.26.2-0ubuntu1 C++ Wrapper for pango (shared libraries)
ii libpaper-utils 1.1.23+nmu1build1 library for handling paper characteristics (utilities)
ii libpaper1 1.1.23+nmu1build1 library for handling paper characteristics
ii libparams-util-perl 1.00-1 Perl extension for simple stand-alone param checking functions
ii libparse-debianchangelog-perl 1.1.1-2ubuntu2 parse Debian changelogs and output them in other formats
ii libparse-recdescent-perl 1.963+dfsg-1 Perl module to create and use recursive-descent parsers
ii libparted0 2.2-5ubuntu5.1 The GNU Parted disk partitioning shared library (old name)
ii libparted0debian1 2.2-5ubuntu5.1 The GNU Parted disk partitioning shared library
ii libpcap-dev 1.0.0-6 development library for libpcap (transitional package)
ii libpcap0.8 1.0.0-6 system interface for user-level packet capture
ii libpcap0.8-dev 1.0.0-6 development library and header files for libpcap0.8
ii libpci3 1:3.0.0-4ubuntu17 Linux PCI Utilities (shared library)
ii libpciaccess0 0.11.0-1 Generic PCI access library for X
ii libpcre3 7.8-3build1 Perl 5 Compatible Regular Expression Library - runtime files
ii libpcsclite1 1.5.3-1ubuntu4.2 Middleware to access a smart card using PC/SC (library)
ii libperl-dev 5.10.1-8ubuntu2.1 Perl library: development files
ii libperl5.10 5.10.1-8ubuntu2.1 shared Perl library
ii libphonon4 4:4.7.0really4.4.2-0ubuntu1~lucid1~ppa1 the core library of the Phonon multimedia framework
ii libpixman-1-0 0.16.4-1ubuntu2 pixel-manipulation library for X and cairo
ii libpixman-1-dev 0.16.4-1ubuntu2 pixel-manipulation library for X and cairo (development files)
ii libpkcs11-helper1 1.07-1build1 library that simplifies the interaction with PKCS#11
ii libplasma-geolocation-interface4 4:4.5.3-0ubuntu1~lucid1~ppa1 library for the Plasma geolocation
ii libplasma3 4:4.5.3-0ubuntu1~lucid1~ppa2 the Plasma Library for the KDE Platform
ii libplasmaclock4b 4:4.5.3-0ubuntu1~lucid1~ppa1 library for Plasma clocks
ii libplasmagenericshell4 4:4.5.3-0ubuntu1~lucid1~ppa1 shared elements for all the plasma shells
ii libplist1 1.1-1ubuntu1 Library for handling Apple binary and XML property lists
ii libplrpc-perl 0.2020-2 Perl extensions for writing PlRPC servers and clients
ii libplymouth2 0.8.2-2ubuntu2.2 graphical boot animation and logger - shared libraries
ii libpng12-0 1.2.42-1ubuntu2.1 PNG library - runtime
ii libpng12-dev 1.2.42-1ubuntu2.1 PNG library - development
ii libpolkit-agent-1-0 0.96-2ubuntu0.1 PolicyKit Authentication Agent API
ii libpolkit-backend-1-0 0.96-2ubuntu0.1 PolicyKit backend API
ii libpolkit-gobject-1-0 0.96-2ubuntu0.1 PolicyKit Authorization API
ii libpolkit-qt-1-0 0.95.1-1fakesync1 PolicyKit-qt-1 library
ii libpoppler-glib4 0.12.4-0ubuntu5.1 PDF rendering library (GLib-based shared library)
ii libpoppler-qt4-3 0.12.4-0ubuntu5.1 PDF rendering library (Qt 4 based shared library)
ii libpoppler5 0.12.4-0ubuntu5.1 PDF rendering library
ii libpopt0 1.15-1 lib for parsing cmdline parameters
ii libportaudio0 18.1-7.1 Portable audio I/O - shared library
ii libportaudio2 19+svn20090620-0ubuntu2 Portable audio I/O - shared library
ii libpostproc51 4:0.5.1-1ubuntu1.1 ffmpeg video postprocessing library

ii libpq5 8.4.8-0ubuntu0.10.04 PostgreSQL C client library
ii libprelude2 1.0.0~rc1-1 Security Information Management System [Base library]
ii libprocesscore4a 4:4.5.3-0ubuntu1~lucid1~ppa1 library for ksysguard based process view
ii libprocessui4a 4:4.5.3-0ubuntu1~lucid1~ppa1 library for ksysguard process user interface
ii libprotobuf5 2.2.0a-0.1ubuntu1 protocol buffers C++ library
ii libproxy0 0.3.1-1ubuntu1 automatic proxy configuration management library (shared)
ii libpst4 0.6.41-0ubuntu4 Shared library needed by the readpst utilities, and
ii libpth20 2.0.7-14 The GNU Portable Threads
ii libpthread-stubs0 0.3-2 pthread stubs not provided by native libc
ii libpthread-stubs0-dev 0.3-2 pthread stubs not provided by native libc, development files
ii libpulse-mainloop-glib0 1:0.9.22~0.9.21+stable-queue-32-g8478-0ubuntu14.1 PulseAudio client libraries (glib support)
ii libpulse0 1:0.9.22~0.9.21+stable-queue-32-g8478-0ubuntu14.1 PulseAudio client libraries
ii libpurple-bin 1:2.6.6-1ubuntu4.3 multi-protocol instant messaging library - extra utilities
ii libpurple0 1:2.6.6-1ubuntu4.3 multi-protocol instant messaging library
ii libpython2.6 2.6.5-1ubuntu6 Shared Python runtime library (version 2.6)
ii libqalculate4 0.9.6-4ubuntu2 Powerful and easy to use desktop calculator - library
ii libqca2 2.0.2-1ubuntu2 libraries for the Qt Cryptographic Architecture
ii libqgpgme1 4:4.5.3-0ubuntu1~lucid1~ppa1 library for GpgME++ integration with Qt
ii libqimageblitz4 1:0.0.4-4build1 QImageBlitz image effects library
ii libqt3-mt 3:3.3.8-b-6ubuntu2 Qt GUI Library (Threaded runtime version), Version 3
ii libqt4-core 4:4.7.0-0ubuntu2~lucid1~ppa2 transitional package for Qt 4 core non-GUI runtime libraries
ii libqt4-dbus 4:4.7.0-0ubuntu2~lucid1~ppa2 Qt 4 D-Bus module
ii libqt4-designer 4:4.7.0-0ubuntu2~lucid1~ppa2 Qt 4 designer module
ii libqt4-help 4:4.7.0-0ubuntu2~lucid1~ppa2 Qt 4 help module
ii libqt4-network 4:4.7.0-0ubuntu2~lucid1~ppa2 Qt 4 network module
ii libqt4-opengl 4:4.7.0-0ubuntu2~lucid1~ppa2 Qt 4 OpenGL module
ii libqt4-qt3support 4:4.7.0-0ubuntu2~lucid1~ppa2 Qt 3 compatibility library for Qt 4
ii libqt4-script 4:4.7.0-0ubuntu2~lucid1~ppa2 Qt 4 script module
ii libqt4-scripttools 4:4.7.0-0ubuntu2~lucid1~ppa2 Qt 4 script tools module
ii libqt4-sql 4:4.7.0-0ubuntu2~lucid1~ppa2 Qt 4 SQL module
ii libqt4-sql-mysql 4:4.7.0-0ubuntu2~lucid1~ppa2 Qt 4 MySQL database driver
ii libqt4-sql-sqlite 4:4.7.0-0ubuntu2~lucid1~ppa2 Qt 4 SQLite 3 database driver
ii libqt4-svg 4:4.7.0-0ubuntu2~lucid1~ppa2 Qt 4 SVG module
ii libqt4-test 4:4.7.0-0ubuntu2~lucid1~ppa2 Qt 4 test module
ii libqt4-webkit 4:4.7.0-0ubuntu2~lucid1~ppa2 transitional package for Qt 4 WebKit module
ii libqt4-xml 4:4.7.0-0ubuntu2~lucid1~ppa2 Qt 4 XML module
ii libqt4-xmlpatterns 4:4.7.0-0ubuntu2~lucid1~ppa2 Qt 4 XML patterns module
ii libqtcore4 4:4.7.0-0ubuntu2~lucid1~ppa2 Qt 4 core module
ii libqtgui4 4:4.7.0-0ubuntu2~lucid1~ppa2 Qt 4 GUI module
ii libqtwebkit4 2.0.0-0ubuntu1~lucid1~ppa1 Web content engine library for Qt
ii libquicktime1 2:1.1.4-1 library for reading and writing Quicktime files
ii libqwt5-qt4 5.2.0-1build1 Qt4 widgets library for technical applications (runtime)
ii libraptor1 1.4.21-1ubuntu1 Raptor RDF parser and serializer library
ii librarian0 0.8.1-4ubuntu1 Documentation meta-data library (library package)
ii librasqal2 0.9.17-1 Rasqal RDF query library
ii libraw1394-11 2.0.4-1ubuntu2 library for direct access to IEEE 1394 bus (aka FireWire)

ii librdf0 1.0.10-1ubuntu1 Redland Resource Description Framework (RDF) library
ii libreadline-ruby 4.2-2~uorppa0 Readline interface for Ruby
ii libreadline-ruby1.8 1.8.7.249-2 Readline interface for Ruby 1.8
ii libreadline-ruby1.9.2 1.9.2.z1-1ppa1~lucid Readline interface for Ruby 1.9.2
ii libreadline5 5.2-7build1 GNU readline and history libraries, run-time libraries
ii libreadline5-dev 5.2-7build1 GNU readline and history libraries, development files
ii libreadline6 6.1-1 GNU readline and history libraries, run-time libraries
ii libreadonly-perl 1.03-2 Facility for creating read-only scalars, arrays and hashes
ii libreadonly-xs-perl 1.04-2 Faster Readonly implementation
ii librecode0 3.6-17 Shared library on which recode is based
ii libregexp-java 1.5-2 Regular expression library for Java
ii libreoffice 1:3.3.2-1ubuntu2~lucid1 office productivity suite
ii libreoffice-base 1:3.3.2-1ubuntu2~lucid1 office productivity suite -- database
ii libreoffice-base-core 1:3.3.2-1ubuntu2~lucid1 office productivity suite -- shared library
ii libreoffice-calc 1:3.3.2-1ubuntu2~lucid1 office productivity suite -- spreadsheet
ii libreoffice-common 1:3.3.2-1ubuntu2~lucid1 office productivity suite -- arch-independent files
ii libreoffice-core 1:3.3.2-1ubuntu2~lucid1 office productivity suite -- arch-dependent files
ii libreoffice-draw 1:3.3.2-1ubuntu2~lucid1 office productivity suite -- drawing
ii libreoffice-emailmerge 1:3.3.2-1ubuntu2~lucid1 office productivity suite -- email mail merge
ii libreoffice-filter-mobiledev 1:3.3.2-1ubuntu2~lucid1 office productivity suite -- mobile devices filters
ii libreoffice-impress 1:3.3.2-1ubuntu2~lucid1 office productivity suite -- presentation
ii libreoffice-java-common 1:3.3.2-1ubuntu2~lucid1 office productivity suite -- arch-independent Java support files
ii libreoffice-l10n-ar 1:3.3.2-1ubuntu2~lucid1 office productivity suite -- Arabic language package
ii libreoffice-l10n-common 1:3.3.2-1ubuntu2~lucid1 common files for LibreOffice language and help packages
ii libreoffice-l10n-ja 1:3.3.2-1ubuntu2~lucid1 office productivity suite -- Japanese language package
ii libreoffice-math 1:3.3.2-1ubuntu2~lucid1 office productivity suite -- equation editor
ii libreoffice-report-builder-bin 1:3.3.2-1ubuntu2~lucid1 LibreOffice extension for building database reports -- libraries
ii libreoffice-style-human 1:3.3.2-1ubuntu2~lucid1 office productivity suite -- Crystal symbol style
ii libreoffice-writer 1:3.3.2-1ubuntu2~lucid1 office productivity suite -- word processor
ii libresid-builder0c2a 2.1.1-8 SID chip emulation class based on resid
ii librpc-xml-perl 0.72-1 Perl module implementation of XML-RPC
ii librpcsecgss3 0.19-2 allows secure rpc communication using the rpcsec_gss protocol
ii librpm0 4.7.2-1lbuild1 RPM shared library
ii librpmio0 4.7.2-1lbuild1 RPM IO shared library
ii librrd4 1.3.8-1ubuntu1 Time-series data storage and display system (runtime library)
ii librsvg2-2 2.26.3-0ubuntu1 SAX-based renderer library for SVG files (runtime)
ii librsvg2-common 2.26.3-0ubuntu1 SAX-based renderer library for SVG files (extra runtime)
ii libruby1.8 1.8.7.249-2 Libraries necessary to run Ruby 1.8

ii libruby1.9.2 1.9.2.z1-1ppa1~lucid Libraries necessary to run Ruby 1.9.2
ii libruli4 0.33-1.1 Library for easily querying DNS SRV records
ii libsamplerate0 0.1.7-3 Audio sample rate conversion library
ii libsasl2-2 2.1.23.dfsg1-5ubuntu1 Cyrus SASL - authentication abstraction library
ii libsasl2-modules 2.1.23.dfsg1-5ubuntu1 Cyrus SASL - pluggable authentication modules
ii libschroedinger-1.0-0 1.0.9.is.1.0.8-0ubuntu1 library for encoding/decoding of Dirac video streams
ii libscope-guard-perl 0.03-2 lexically scoped resource management
ii libsdl-image1.2 1.2.10-1 image loading library for Simple DirectMedia Layer 1.2
ii libsdl-ttf2.0-0 2.0.9-1build1 ttf library for Simple DirectMedia Layer with FreeType 2 support
ii libsdl1.2debian 1.2.14-4ubuntu1.1 Simple DirectMedia Layer
ii libsdl1.2debian-alsa 1.2.14-4ubuntu1.1 Simple DirectMedia Layer (with X11 and ALSA options)
ii libselinux1 2.0.89-4 SELinux runtime shared libraries
ii libsensors4 1:3.1.2-2 library to read temperature/voltage/fan sensors
ii libsepol1 2.0.40-2 SELinux library for manipulating binary security policies
ii libservlet2.4-java 5.0.30-10 Servlet 2.4 and JSP 2.0 Java library
ii libservlet2.5-java 6.0.24-2ubuntu1.7 Servlet 2.5 and JSP 2.1 Java API classes
ii libsexy2 0.1.11-2build2 collection of additional GTK+ widgets - library
ii libsgutils2-2 1.28-2 utilities for working with generic SCSI devices (shared libraries)
ii libshout3 2.2.2-5ubuntu1 MP3/Ogg Vorbis broadcast streaming library
ii libsidplay1 1.36.59-5 SID (MOS 6581) emulation library
ii libsidplay2 2.1.1-8 SID (MOS 6581) emulation library
ii libsigc++-2.0-0c2a 2.2.4.2-1 type-safe Signal Framework for C++ - runtime
ii libsilc-1.1-2 1.1.10-2build1 SILC generic library
ii libsilcclient-1.1-3 1.1.10-2build1 SILC client library
ii libslang2 2.2.2-2ubuntu1 The S-Lang programming library - runtime version
ii libslf4j-java 1.5.10-1 Simple Logging Facade for Java
ii libslp1 1.2.1-7.6ubuntu0.1 OpenSLP libraries
ii libsm-dev 2:1.1.1-1 X11 Session Management library (development headers)
ii libsm6 2:1.1.1-1 X11 Session Management library
ii libsmbclient 2:3.4.7~dfsg-1ubuntu3.6 shared library for communication with SMB/CIFS servers
ii libsmi2-common 0.4.8+dfsg2-2 a library to access SMI MIB information - MIB module files
ii libsmi2ldbl 0.4.8+dfsg2-2 library to access SMI MIB information
ii libsndfile1 1.0.21-2 Library for reading/writing audio files
ii libsnmp-base 5.4.2.1~dfsg0ubuntu1-0ubuntu2.1 SNMP (Simple Network Management Protocol) MIBs and documentation
ii libsnmp15 5.4.2.1~dfsg0ubuntu1-0ubuntu2.1 SNMP (Simple Network Management Protocol) library
ii libsolid4 4:4.5.3-0ubuntu1~lucid1~ppa2 Solid Library for KDE Platform
ii libsolidcontrol4a 4:4.5.3-0ubuntu1~lucid1~ppa1 library for Solid based network management
ii libsolidcontrolifaces4 4:4.5.3-0ubuntu1~lucid1~ppa1 library for Solid based network interface management
ii libsoprano4 2.5.0+dfsg.1-1ubuntu1~lucid1~ppa2 libraries for the Soprano RDF framework
ii libsoundtouch1c2 1.3.1-2 sound stretching library

ii libsoup-gnome2.4-1 2.30.2-0ubuntu0.1 an HTTP library implementation in C -- GNOME support library
ii libsoup2.4-1 2.30.2-0ubuntu0.1 an HTTP library implementation in C -- Shared library
ii libsox-fmt-all 14.3.0-1.1build1 All SoX format libraries
ii libsox-fmt-alsa 14.3.0-1.1build1 SoX alsa format I/O library
ii libsox-fmt-ao 14.3.0-1.1build1 SoX Libao format I/O library
ii libsox-fmt-base 14.3.0-1.1build1 Minimal set of SoX format libraries
ii libsox-fmt-ffmpeg 14.3.0-1.1build1 SoX ffmpeg format library
ii libsox-fmt-mp3 14.3.0-1.1build1 SoX MP3 format library
ii libsox-fmt-oss 14.3.0-1.1build1 SoX OSS format I/O library
ii libsox-fmt-pulse 14.3.0-1.1build1 SoX PulseAudio format I/O library
ii libsox1a 14.3.0-1.1build1 SoX library of audio effects and processing
ii libspectre1 0.2.3-2 Library for rendering PostScript documents
ii libspeex1 1.2~rc1-1ubuntu1 The Speex codec runtime library
ii libspeexdsp1 1.2~rc1-1ubuntu1 The Speex extended runtime library
ii libspreadsheet-parseexcel-perl 0.5700-1 Perl module to access information from Excel Spreadsheets
ii libspreadsheet-writeexcel-perl 2.36-1 module to create Excel spreadsheets
ii libsql-translator-perl 0.11003-1 SQL translation library
ii libsqlite0 2.8.17-6build2 SQLite shared library
ii libsqlite3-0 3.6.22-1 SQLite 3 shared library
ii libsqlite3-dev 3.6.22-1 SQLite 3 development files
ii libsqlite3-ruby 1.2.4-2.1 SQLite3 interface for Ruby
ii libsqlite3-ruby1.8 1.2.4-2.1 SQLite3 interface for Ruby 1.8
ii libss2 1.41.11-1ubuntu2.1 command-line interface parsing library
ii libssh-4 0.4.2-1ubuntu1 A tiny C SSH library
ii libssh2-1 1.2.2-1 SSH2 client-side library
ii libssl0.9.8 0.9.8k-7ubuntu8.6 SSL shared libraries
ii libstartup-notification0 0.10-1build1 library for program launch feedback (shared library)
ii libstdc++6 4.4.3-4ubuntu5 The GNU Standard C++ Library v3
ii libstdc++6-4.4-dev 4.4.3-4ubuntu5 The GNU Standard C++ Library v3 (development files)
ii libstlport4.6ldbl 4.6.2-7 STLport C++ class library
ii libstreamanalyzer0 0.7.2-0ubuntu1 streamanalyzer library for Strigi Desktop Search
ii libstreams0 0.7.2-0ubuntu1 streams library for for Strigi Desktop Search
ii libstree 0.4.3-bt0 A generic suffix tree library.
ii libsub-exporter-perl 0.981-1 sophisticated exporter for custom-built routines
ii libsub-install-perl 0.924-2 Install subroutines into packages easily
ii libsub-name-perl 0.04-1build1 Assigns a new name to referenced sub
ii libsub-uplevel-perl 0.2200-1 module to spoof the Perl call stack
ii libsvga1 1:1.4.3-29 console SVGA display libraries
ii libsvn1 1.6.6dfsg-2ubuntu1.2 Shared libraries used by Subversion
ii libswscale0 4:0.5.1-1ubuntu1.1 ffmpeg video scaling library
ii libsybdb5 0.82-6build1 libraries for connecting to MS SQL and Sybase SQL servers
ii libsyndication4 4:4.5.3-0ubuntu1~lucid1~ppa1 parser library for RSS and Atom feeds
ii libsys-hostname-long-perl 1.4-2 Figure out the long (fully-qualified) hostname
ii libsysfs-dev 2.1.0-6 interface library to sysfs - development files
ii libsysfs2 2.1.0-6 interface library to sysfs
ii libt1-5 5.1.2-3build1 Type 1 font rasterizer library - runtime

ii libtag1-vanilla 1.6.3-0ubuntu1 TagLib Audio Meta-Data Library (Vanilla flavour)
ii libtag1c2a 1.6.3-0ubuntu1 TagLib Audio Meta-Data Library
ii libtalloc2 2.0.1-1 hierarchical pool based memory allocator
ii libtar 1.2.11-6 C library for manipulating tar archives
ii libtask-weaken-perl 1.03-1 Ensure that a platform has weaken support
ii libtaskmanager4a 4:4.5.3-0ubuntu1~lucid1~ppa1 library which provides task management facilities
ii libtasn1-3 2.4-1 Manage ASN.1 structures (runtime)
ii libtasn1-3-dev 2.4-1 Manage ASN.1 structures (development)
ii libtdb1 1.2.0-1 Trivial Database - shared library
ii libtemplate-perl 2.20-1build1 template processing system written in perl
ii libterm-readkey-perl 2.30-4build1 A perl module for simple terminal control
ii libterm-readline-gnu-perl 1.19-2 Perl extension for the GNU Readline/History Library
ii libtest-exception-perl 0.29-1 module for testing exception-based code
ii libtext-charwidth-perl 0.04-6 get display widths of characters on the terminal
ii libtext-csv-perl 1.16-1 comma-separated values manipulator (using XS or PurePerl)
ii libtext-csv-xs-perl 0.70-1 Perl C/XS module to process Comma-Separated Value files
ii libtext-glob-perl 0.08-2 Perl module for matching globbing patterns against text
ii libtext-iconv-perl 1.7-2 converts between character sets in Perl
ii libtext-recordparser-perl 1.3.0-1 Perl module to parse record-oriented data in a text file
ii libtext-tabulardisplay-perl 1.22-1 Perl module to display text as a formatted table
ii libtext-wrapi18n-perl 0.06-7 internationalized substitute of Text::Wrap
ii libthai-data 0.1.13-1build1 Data files for Thai language support library
ii libthai0 0.1.13-1build1 Thai language support library
ii libtheora0 1.1.1+dfsg.1-3 The Theora Video Compression Codec
ii libthreadweaver4 4:4.5.3-0ubuntu1~lucid1~ppa2 the ThreadWeaver Library for the KDE Platform
ii libthunar-vfs-1-2 1.0.1-3ubuntu1 VFS abstraction used in thunar
ii libtidy-0.99-0 20091223cvs-1 HTML syntax checker and reformatter - library
ii libtie-ixhash-perl 1.21-2 ordered associative arrays for Perl
ii libtiff4 3.9.2-2ubuntu0.7 Tag Image File Format (TIFF) library
ii libtimedate-perl 1.1900-1 Time and date functions for Perl
ii libtommath0 0.39-3ubuntu1 multiple-precision integer library [runtime]
ii libtool 2.2.6b-2ubuntu1 Generic library support script
ii libtotem-plparser17 2.30.0git201000413-0ubuntu1 Totem Playlist Parser library - runtime files
ii libtre5 0.8.0-2 regexp matching library with approximate matching
ii libtry-tiny-perl 0.04-1 module providing minimalistic try/catch
ii libts-0.0-0 1.0-7build1 touch screen library
ii libtwolame0 0.3.12-1 MPEG Audio Layer 2 encoding library
ii libudev0 151-12.3 udev library
ii libumfpack5.4.0 1:3.4.0-1ubuntu3 sparse LU factorization library
ii libunicode-map-perl 0.112-10build1 Perl module for mapping charsets from and to UTF16 Unicode
ii libuniconf4.6 4.6.1-1 C++ network libraries for rapid application development
ii libunique-1.0-0 1.1.6-1ubuntu2 Library for writing single instance applications - shared libraries
ii libupnp3 1:1.6.6-4 Portable SDK for UPnP Devices, version 1.6 (shared libraries)

ii libupower-glib1 0.9.1-1 abstraction for power management - shared library
ii liburi-perl 1.52-1 module to manipulate and access URI strings
ii libusb-0.1-4 2:0.1.12-14ubuntu0.2 userspace USB programming library
ii libusb-1.0-0 2:1.0.6-1 userspace USB programming library
ii libusbmuxd1 1.0.2-1ubuntu2 USB multiplexor daemon for iPhone and iPod Touch devices - library
ii libusplash-dev 0.5.51 Theming support files for usplash
ii libusplash0 0.5.51 userspace bootsplash library
ii libutempter0 1.1.5-2 A privileged helper for utmp/wtmp updates (runtime)
ii libuuid-perl 0.02-3build2 Perl extension for using UUID interfaces as defined in e2fsprogs
ii libuuid1 2.17.2-0ubuntu1.10.04.2 Universally Unique ID library
ii libv4l-0 0.6.4-1ubuntu1 Collection of video4linux support libraries
ii libv4l-dev 0.6.4-1ubuntu1 Collection of video4linux support libraries (development files)
ii libvamp-hostsdk3 2.1-1 helper library for Vamp hosts written in C++
ii libvcdinfo0 0.7.23-4ubuntu2 library to extract information from VideoCD
ii libvirtodbc0 6.1.2+dfsg1-1ubuntu4~lucid1~ppa1 high-performance database - ODBC libraries
ii libvisual-0.4-0 0.4.0-2.1+ubuntu2 Audio visualization framework
ii libvisual-0.4-plugins 0.4.0.dfsg.1-2ubuntu5 Audio visualization framework plugins
ii libvlc2 1.0.6-1ubuntu1.6 multimedia player and streamer library
ii libvlccore2 1.0.6-1ubuntu1.6 base library for VLC and its modules
ii libvorbis0a 1.2.3-3ubuntu1 The Vorbis General Audio Compression Codec (Decoder library)
ii libvorbisenc2 1.2.3-3ubuntu1 The Vorbis General Audio Compression Codec (Encoder library)
ii libvorbisfile3 1.2.3-3ubuntu1 The Vorbis General Audio Compression Codec (High Level API)
ii libvpx0 0.9.5-2~build0.10.04.1 VP8 video codec (shared library)
ii libvte-common 1:0.23.5-0ubuntu1.1 Terminal emulator widget for GTK+ 2.0 - common files
ii libvte9 1:0.23.5-0ubuntu1.1 Terminal emulator widget for GTK+ 2.0 - runtime files
ii libwavpack1 4.60.1-1 an audio codec (lossy and lossless) - library
ii libwbclient0 2:3.4.7~dfsg-1ubuntu3.6 Samba winbind client library
ii libweather-ion5 4:4.5.3-0ubuntu1~lucid1~ppa1 library which provides an interface for weather information services
ii libwebkit-1.0-2 1.2.5-0ubuntu0.10.04.1 Web content engine library for Gtk+
ii libwebkit-1.0-common 1.2.5-0ubuntu0.10.04.1 Web content engine library for Gtk+ - data files
ii libwhisker2-perl 2.4-1 Perl module geared for HTTP testing
ii libwmf-bin 0.2.8.4-6.1ubuntu2 Windows metafile conversion tools
ii libwmf0.2-7 0.2.8.4-6.1ubuntu2 Windows metafile conversion library
ii libwnck-common 1:2.30.0-0ubuntu1 Window Navigator Construction Kit - common files
ii libwnck22 1:2.30.0-0ubuntu1 Window Navigator Construction Kit - runtime files
ii libwpd8c2a 0.8.14-1build1 Library for handling WordPerfect documents (shared library)
ii libwpg-0.1-1 0.1.3-1build1 WordPerfect graphics import/convert library (shared library)
ii libwrap0 7.6.q-18 Wietse Venema's TCP wrappers library
ii libwvstreams4.6-base 4.6.1-1 C++ network libraries for rapid application development
ii libwvstreams4.6-extras 4.6.1-1 C++ network libraries for rapid application development

ii libwww-mechanize-perl 1.58-1 module to automate interaction with websites
ii libwww-perl 5.834-1ubuntu0.1 Perl HTTP/WWW client/server library
ii libwxbase2.8-0 2.8.10.1-0ubuntu1.2 wxBase library (runtime) - non-GUI support classes of wxWidgets toolkit
ii libwxgtk2.8-0 2.8.10.1-0ubuntu1.2 wxWidgets Cross-platform C++ GUI toolkit (GTK+ runtime)
ii libx11-6 2:1.3.2-1ubuntu3 X11 client-side library
ii libx11-data 2:1.3.2-1ubuntu3 X11 client-side library
ii libx11-dev 2:1.3.2-1ubuntu3 X11 client-side library (development headers)
ii libx264-85 2:0.85.1448+git1a6d32-4 x264 video coding library
ii libx86-1 1.1+ds1-6 x86 real-mode library
ii libxapian15 1.0.18-1 Search engine library
ii libxau-dev 1:1.0.5-1 X11 authorisation library (development headers)
ii libxau6 1:1.0.5-1 X11 authorisation library
ii libxaw7 2:1.0.7-1 X11 Athena Widget library
ii libxcb-atom1 0.3.6-1build1 utility libraries for X C Binding -- atom
ii libxcb-aux0 0.3.6-1build1 utility libraries for X C Binding -- aux
ii libxcb-event1 0.3.6-1build1 utility libraries for X C Binding -- event
ii libxcb-keysyms1 0.3.6-1build1 utility libraries for X C Binding -- keysyms
ii libxcb-render-util0 0.3.6-1build1 utility libraries for X C Binding -- render-util
ii libxcb-render-util0-dev 0.3.6-1build1 utility libraries for X C Binding -- render-util
ii libxcb-render0 1.5-2 X C Binding, render extension
ii libxcb-render0-dev 1.5-2 X C Binding, render extension, development files
ii libxcb-shape0 1.5-2 X C Binding, shape extension
ii libxcb-shm0 1.5-2 X C Binding, shm extension
ii libxcb-xv0 1.5-2 X C Binding, xv extension
ii libxcb1 1.5-2 X C Binding
ii libxcb1-dev 1.5-2 X C Binding, development files
ii libxcomposite-dev 1:0.4.1-1 X11 Composite extension library (development headers)
ii libxcomposite1 1:0.4.1-1 X11 Composite extension library
ii libxcursor-dev 1:1.1.10-1 X cursor management library (development files)
ii libxcursor1 1:1.1.10-1 X cursor management library
ii libxdamage-dev 1:1.1.2-1 X11 damaged region extension library (development headers)
ii libxdamage1 1:1.1.2-1 X11 damaged region extension library
ii libxdmcp-dev 1:1.0.3-1 X11 authorisation library (development headers)
ii libxdmcp6 1:1.0.3-1 X11 Display Manager Control Protocol library
ii libxerces2-java 2.9.1-4ubuntu1 Validating XML parser for Java with DOM level 3 support
ii libxext-dev 2:1.1.1-2 X11 miscellaneous extensions library (development headers)
ii libxext6 2:1.1.1-2 X11 miscellaneous extension library
ii libxfce4util-bin 4.6.1-2ubuntu2 tools for libxfce4util
ii libxfce4util-common 4.6.1-2ubuntu2 common files for libxfce4util
ii libxfce4util4 4.6.1-2ubuntu2 Utility functions library for Xfce4
ii libxfcegui4-4 4.6.3-2 Basic GUI C functions for Xfce4
ii libxfconf-0-2 4.6.1-2ubuntu2 Client library for Xfce4 configure interface
ii libxfixes-dev 1:4.0.4-1 X11 miscellaneous 'fixes' extension library (development headers)
ii libxfixes3 1:4.0.4-1 X11 miscellaneous 'fixes' extension library
ii libxfont1 1:1.4.1-1 X11 font rasterisation library
ii libxft-dev 2.1.14-1ubuntu1 FreeType-based font drawing library for X (development files)

ii libxft2 2.1.14-1ubuntu1 FreeType-based font drawing library for X
ii libxi-dev 2:1.3-3 X11 Input extension library (development headers)
ii libxi6 2:1.3-3 X11 Input extension library
ii libxine1 1.1.17-1ubuntu3 the xine video/media player library, meta-package
ii libxine1-bin 1.1.17-1ubuntu3 the xine video/media player library, binary files
ii libxine1-console 1.1.17-1ubuntu3 libaa/libcaca/framebuffer/directfb related plugins for libxine1
ii libxine1-ffmpeg 1.1.17-1ubuntu3 MPEG-related plugins for libxine1
ii libxine1-misc-plugins 1.1.17-1ubuntu3 Input, audio output and post plugins for libxine1
ii libxine1-x 1.1.17-1ubuntu3 X desktop video output plugins for libxine1
ii libxinerama-dev 2:1.1-2 X11 Xinerama extension library (development headers)
ii libxinerama1 2:1.1-2 X11 Xinerama extension library
ii libxkbfile1 1:1.0.6-1 X11 keyboard file manipulation library
ii libxklavier16 5.0-0ubuntu1 X Keyboard Extension high-level API
ii libxml-dom-perl 1.44-1 Perl module for building DOM Level 1 compliant doc structures
ii libxml-libxml-perl 1.70.ds-1 Perl interface to the libxml2 library
ii libxml-namespacesupport-perl 1.09-3 Perl module for supporting simple generic namespaces
ii libxml-parser-perl 2.36-1.1build3 Perl module for parsing XML files
ii libxml-perl 0.08-2 Perl modules for working with XML
ii libxml-regexp-perl 0.03-8 Perl module for regular expressions for XML tokens
ii libxml-sax-expat-perl 0.40-1 Perl module for a SAX2 driver for Expat (XML::Parser)
ii libxml-sax-perl 0.96+dfsg-2 Perl module for using and building Perl SAX2 XML processors
ii libxml-simple-perl 2.18-3 Perl module for reading and writing XML
ii libxml-twig-perl 1:3.32-3ubuntu1 Perl module for processing huge XML documents in tree mode
ii libxml-writer-perl 0.605-1 Perl module for writing XML documents
ii libxml-xpath-perl 1.13-7 Perl module for processing XPath
ii libxml2 2.7.6.dfsg-1ubuntu1.1 GNOME XML library
ii libxml2-dev 2.7.6.dfsg-1ubuntu1.1 Development files for the GNOME XML library
ii libxml2-doc 2.7.6.dfsg-1ubuntu1.1 Documentation for the GNOME XML library
ii libxml2-utils 2.7.6.dfsg-1ubuntu1.1 XML utilities
ii libxmu6 2:1.0.5-1 X11 miscellaneous utility library
ii libxmuu1 2:1.0.5-1 X11 miscellaneous micro-utility library
ii libxp6 1:1.0.0.xsf1-2build1 X Printing Extension (Xprint) client library
ii libxpm4 1:3.5.8-1 X11 pixmap library
ii libxrandr-dev 2:1.3.0-3 X11 RandR extension library (development headers)
ii libxrandr2 2:1.3.0-3 X11 RandR extension library
ii libxrender-dev 1:0.9.5-1 X Rendering Extension client library (development files)
ii libxrender1 1:0.9.5-1 X Rendering Extension client library
ii libxres1 2:1.0.4-1 X11 Resource extension library
ii libxslt1-dev 1.1.26-1ubuntu1 XSLT processing library - development kit
ii libxslt1.1 1.1.26-1ubuntu1 XSLT processing library - runtime library
ii libxss1 1:1.2.0-2 X11 Screen Saver extension library
ii libxt-dev 1:1.0.7-1 X11 toolkit intrinsics library (development headers)
ii libxt6 1:1.0.7-1 X11 toolkit intrinsics library
ii libxtst6 2:1.1.0-2 X11 Testing -- Resource extension library
ii libxv1 2:1.0.5-1 X11 Video extension library

ii libxvidcore4 2:1.2.2+debian-0ubuntu2 An open source MPEG-4 video codec (library)
ii libxvmc1 2:1.0.5-1ubuntu1 X11 Video extension library
ii libxxf86dga1 2:1.1.1-2 X11 Direct Graphics Access extension library
ii libxxf86vm1 1:1.1.0-2 X11 XFree86 video mode extension library
ii libyaml-0-2 0.1.3-1 Fast YAML 1.1 parser and emitter library
ii libyaml-perl 0.71-1 YAML Ain't Markup Language
ii libyaml-syck-perl 1.07-1build1 fast, lightweight YAML loader and dumper
ii libzephyr4 3.0-1 Project Athena's notification service - non-Kerberos libraries
ii linux-firmware 2.0-bt5 Linux Kernel Firmware
ii linux-headers 1.1-bt3 BackTrack Linux Kernel Headers Virtual Package
ii linux-headers-2.6.39.4 2.6.39.4-10.00.Custom Header files related to Linux kernel, specifically,
ii linux-image 1.1-bt3 BackTrack Linux Kernel Image Virtual Package
ii linux-image-2.6.39.4 2.6.39.4-10.00.Custom Linux kernel binary image for version 2.6.39.4
ii linux-libc-dev 2.6.32-29.58 Linux Kernel Headers for development
ii linux-sound-base 1.0.22.1+dfsg-0ubuntu3 base package for ALSA and OSS sound systems
ii linux-source 1.1-bt3 BackTrack Linux Kernel Source Virtual Package
ii linux-source-2.6.39.4 2.6.39.4-10.00.Custom Linux kernel source for version 2.6.39.4
ii list-urls 3.0-bt2 Extract URLS from a web page.
ii lm-sensors 1:3.1.2-2 utilities to read temperature/voltage/fan sensors
ii lmodern 2.004.1-3 scalable PostScript and OpenType fonts based on Computer Modern
ii localechooser-data 2.12ubuntu3 Lists of locales supported by the installer
ii localepurge 0.6.2 Reclaim disk space removing unneeded localizations
ii locales 2.11+git20100304-3 common files for locale support
ii lockfile-progs 0.1.13ubuntu1 Programs for locking and unlocking files and mailboxes
ii login 1:4.1.4.2-1ubuntu2.2 system login tools
ii logrotate 3.7.8-4ubuntu2.1 Log rotation utility
ii lp-solve 5.5.0.13-7 Solve (mixed integer) linear programming problems
ii lsb-base 4.0-0ubuntu8 Linux Standard Base 4.0 init script functionality
ii lsb-release 4.0-0ubuntu8 Linux Standard Base version reporting utility
ii lshw 02.14-1build1 information about hardware configuration
ii lsof 4.81.dfsg.1-1build1 List open files
ii ltrace 0.5.3-2ubuntu3 Tracks runtime library calls in dynamically linked programs
ii luatex 0.50.0-1 next generation TeX engine
ii lxsplit 0.2.4-0ubuntu1 This program is a simple tool for splitting and joining files
ii lynx 2.8.8dev.2-1 Text-mode WWW Browser (transitional package)
ii lynx-cur 2.8.8dev.2-1 Text-mode WWW Browser with NLS support (development version)
ii lzma 4.43-14ubuntu2 Compression method of 7z format in 7-Zip program
ii m4 1.4.13-3 a macro processing language
ii macchanger 1.5.0-bt2 A GNU/Linux utility for viewing/manipulating the MAC address of network interfaces.
ii magicrescue 1.19-bt0 Scans a block device for file types it knows how to recover and calls an external program to extract them.
ii magictree r1492-bt1 A penetration tester productivity tool which allows easy and straightforward data consolidation
ii make 3.81-7ubuntu1 An utility for Directing compilation.
ii makedev 2.3.1-89ubuntu1 creates device files in /dev

ii maltego 3.0-bt4 OSINT software
ii man-db 2.5.7-2ubuntu1 on-line manual pager
ii manpages 3.23-1 Manual pages about using a GNU/Linux system
ii manpages-dev 3.23-1 Manual pages about using GNU/Linux for development
ii mantra 0.71-bt0 Mantra is a security framework which can be very helpful in performing all the five phases of attacks including reconnaissance, scanning and enumeration,
ii marble-data 4:4.5.3-0ubuntu1~lucid1~ppa3 data files for Marble
ii marble-plugins 4:4.5.3-0ubuntu1~lucid1~ppa3 plugins for Marble
ii mawk 1.3.3-15ubuntu2 a pattern scanning and text processing language
ii md5deep 3.4-bt0 A set of programs to compute MD5, SHA-1, SHA-256, Tiger, or Whirlpool message digests on an arbitrary number of files.
ii mdbtools 0.5.99.0.6pre1.0.20051109-6 JET / MS Access database (MDB) tools
ii mdk3 6.0-bt1 MDK is a proof-of-concept tool to exploit common IEEE 802.11 protocol weaknesses using the oslib of aircrack-ng.
ii medusa 2.0-bt4 parallel network login auditor
ii melt 0.5.4-1 command line media player and video editor
ii memtest86+ 4.00-2ubuntu3 thorough real-mode memory tester
ii mencoder 2:1.0~rc3+svn20090426-1ubuntu16.1 MPlayer's Movie Encoder
ii menu 2.1.43ubuntu1 generates programs menu for all menu-aware applications
ii mesa-utils 7.7.1-1ubuntu3 Miscellaneous Mesa GL utilities
ii metacity-common 1:2.30.1-0ubuntu1.1 shared files for the Metacity window manager
ii metagoofil 2.1-bt0 Metagoofil is a tool for extracting metadata of public documents (pdf,doc,xls,ppt) availables in the target websites.
ii mime-support 3.48-1ubuntu1 MIME files 'mime.types' & 'mailcap', and support programs
ii min12xxw 0.0.9-3ubuntu2 Printer driver for KonicaMinolta PagePro 1[234]xxW
ii mingw 3.14-bt0 A minimalist development environment for native Microsoft Windows applications.
ii miranda 1.0-bt0 Miranda is a Python-based Universal Plug-N-Play client application designed to discover, query and interact with UPNP devices, particularly Internet Gatew
ii miredo 1.2.3-bt5 Miredo is an open-source Teredo IPv6 tunneling software, for Linux and the BSD operating systems. It includes functional implementations of all components
ii missidentify 1.0-bt0 Miss Identify is a program to find Win32 applications.
ii mjpegtools 1:1.9.0-0.5ubuntu3 MJPEG video capture/editting/playback MPEG encoding
ii mktemp 7.4-2ubuntu3 coreutils mktemp transitional package
ii mlocate 0.22.2-1ubuntu1 quickly find files on the filesystem based on their name
ii module-init-tools 3.11.1-2ubuntu1 tools for managing Linux kernel modules
ii mopest 2.0-bt0 PHP web vulnerability scanner.
ii mork.pl 1.0-bt0 This script lets you extract the URLs from your Mozilla history file, sorted by last access time.
ii mount 2.17.2-0ubuntu1.10.04.2 Tools for mounting and manipulating filesystems
ii mountall 2.15.3 filesystem mounting tool
ii mp3blaster 1:3.2.5-2 Full-screen console mp3 and Ogg Vorbis player
ii mp3splt 2.2.5-1 command line interface to split MP3 and Ogg Vorbis files without reencoding
ii mp3wrap 0.5-3 Utility for MP3 wrapping (rolling multiple MP3s into one)
ii mpg123 1.12.1-0ubuntu1 MPEG layer 1/2/3 audio player
ii mplayer 2:1.0~rc3+svn20090426-1ubuntu16.1 movie player for Unix-like systems
ii mscompress 0.3-3build1 Microsoft "compress.exe/expand.exe" compatible

(de)compressor
ii mtools 4.0.10-1ubuntu1 Tools for manipulating MSDOS files
ii mtr-tiny 0.75-2build1 Full screen ncurses traceroute tool
ii multisystem 1.0167 Avec MultiSystem Cr ez votre LiveUSB MultiBoot simplement,
ii myspell-en-au 2.1-5 English_australian dictionary for myspell
ii myspell-en-gb 1:3.2.0-3ubuntu3.1 English_british dictionary for myspell
ii myspell-en-za 1:3.2.0-3ubuntu3.1 English_southafrican dictionary for myspell
ii mysql-client-5.1 5.1.41-3ubuntu12.10 MySQL database client binaries
ii mysql-client-core-5.1 5.1.41-3ubuntu12.10 MySQL database core client binaries
ii mysql-common 5.1.41-3ubuntu12.10 MySQL database common files (e.g.
/etc/mysql/my.cnf)
ii mysql-server 5.1.41-3ubuntu12.10 MySQL database server (metapackage depending on
the latest version)
ii mysql-server-5.1 5.1.41-3ubuntu12.10 MySQL database server binaries
ii mysql-server-core-5.1 5.1.41-3ubuntu12.10 MySQL database core server files
ii nano 2.2.2-1 small, friendly text editor inspired by Pico
ii nasm 2.07-1 General-purpose x86 assembler
ii nbtscan 1.5.1a-bt2 NBTscan is a program for scanning IP networks for NetBIOS name
information.
ii ncrack 0.4-bt0 Ncrack is a high-speed network authentication cracking tool.
ii ncurses-base 5.7+20090803-2ubuntu3 basic terminal type definitions
ii ncurses-bin 5.7+20090803-2ubuntu3 terminal-related programs and man pages
ii ncurses-term 5.7+20090803-2ubuntu3 additional terminal type definitions
ii nessus 4.4.1 Version 4 of the Nessus Scanner
ii net-tools 1.60-23ubuntu2 The NET-3 networking toolkit
ii netbase 4.35ubuntu3 Basic TCP/IP networking system
ii netcat 1.10-38 TCP/IP swiss army knife -- transitional package
ii netcat-traditional 1.10-38 TCP/IP swiss army knife
ii netdiscover 0.3beta6-bt4 Netdiscover is an active/passive address reconnaissance tool,
mainly developed for those wireless networks without dhcp server, when you are
wardriving. I
ii netifera 1.0-bt4 Netifera is a new modular open source platform for creating network
security tools.
ii netmask 2.3.10-bt3 Tool for generating terse netmasks.
ii netpbm 2:10.0-12.1ubuntu1 Graphics conversion tools between image formats
ii network-manager-dev 0.8-0ubuntu3 network management framework (development
files)
ii nfs-common 1:1.2.0-4ubuntu4.1 NFS support files common to client and server
ii ngrep 1.45.ds2-9 grep for network traffic
ii nikto 2.1.4-bt5 Nikto is an Open Source (GPL) web server scanner which performs
comprehensive tests against web servers for multiple items, including over 6400 potentiall
ii nis 3.17-31 clients and daemons for the Network Information Service (NIS)
ii nmap 5.61-bt1 NMAP port and vulnerability scanner
ii notification-daemon 0.4.0-2ubuntu2 a daemon that displays passive pop-up notifications
ii nrg2iso 0.4-4 Extracts ISO9660 data from Nero ".nrg" files
ii ntfs-3g 1:2010.3.6-1ubuntu1 read-write NTFS driver for FUSE
ii ntfsprogs 2.0.0-1ubuntu4 tools for doing neat things in NTFS partitions from Linux
ii ntpdate 1:4.2.4p8+dfsg-1ubuntu2.1 client for setting system time from NTP servers

ii oat 1.3.1-bt2 Toolkit for auditing Oracle databases
ii obex-data-server 0.4.5-1 D-Bus service for OBEX client and server side functionality
ii obexd 0.40-bt0 OBEX connectivity. Client and Server.
ii obexftp 0.23-1 file transfer utility for devices that use the OBEX protocol
ii oclhashcat 0.25-bt0 GPU based password cracker with nvidia and ati support
ii oclhashcat+ 0.07-bt0 GPU based password cracker with crypt md5, DES and Apache MD5 support and a enhanced rule engine.
ii oclhashcat-lite 0.08-bt0 Very fast single hash GPU based password cracker
ii odbcinst 2.2.11-21 Helper program for accessing odbc ini files
ii odbcinst1debian1 2.2.11-21 Support library for accessing odbc ini files
ii ohrwurm 0.1-bt0 ohrwurm is a simple RTP fuzzer.
ii oinkmaster 2.0-2ubuntu1 Snort rules manager
ii okteta 4:4.5.3-0ubuntu1~lucid1~ppa1 hexadecimal editor for binary files for KDE 4
ii okular 4:4.5.3-0ubuntu1~lucid1~ppa1 document viewer for KDE 4
ii ollydbg 2.01-bt2 Windows Debugger Ollydbg 2.01
ii onesixtyone 0.3.2-bt4 Fast SNMP scanner and bruteforce tool
ii openbsd-inetd 0.20080125-4ubuntu2 The OpenBSD Internet Superserver
ii openjdk-6-jdk 6b20-1.9.7-0ubuntu1~10.04.1 OpenJDK Development Kit (JDK)
ii openjdk-6-jre 6b20-1.9.7-0ubuntu1~10.04.1 OpenJDK Java runtime, using Hotspot JIT
ii openjdk-6-jre-headless 6b20-1.9.7-0ubuntu1~10.04.1 OpenJDK Java runtime, using Hotspot JIT (headless)
ii openjdk-6-jre-lib 6b20-1.9.7-0ubuntu1~10.04.1 OpenJDK Java runtime (architecture independent libraries)
ii openmovieeditor 0.0.20080102-2.2ubuntu3 a simple non-linear video editor
ii openprinting-ppds 20100216-0ubuntu3 OpenPrinting printer support - PostScript PPD files
ii openssh-client 1:5.3p1-3ubuntu6 secure shell (SSH) client, for secure access to remote machines
ii openssh-server 1:5.3p1-3ubuntu6 secure shell (SSH) server, for secure access from remote machines
ii openssl 0.9.8k-7ubuntu8.6 Secure Socket Layer (SSL) binary and related cryptographic tools
ii openssl-blacklist 0.5-2 list of blacklisted OpenSSL RSA keys
ii openvas 1.0-bt1 OpenVAS vulnerability assesment suite
ii openvas-administrator 1.1.1-bt2 This is the administrator module for the Open Vulnerability Assessment System (OpenVAS). It is intended to simplify the configuration and administration o
ii openvas-check-setup 2.0.6-bt3 Script for checking the completeness and readiness of OpenVAS. Also provides Guidance in case of problems.
ii openvas-cli 1.1.2-bt1 The module OpenVAS-CLI collects command line tools to handle with the OpenVAS services via the respective protocols.
ii openvas-libraries 4.0.5-bt0 This is the libraries module for the Open Vulnerability Assessment System (OpenVAS)
ii openvas-manager 2.0.4-bt1 The OpenVAS Manager is a layer between the OpenVAS Scanner and various client applications such as the web client GSA (Greenbone Security Assistant), the
ii openvas-scanner 3.2.3-bt4 This is the scanner module for the Open Vulnerability Assessment System
ii openvpn 2.1.0-1ubuntu1.1 virtual private network daemon

ii openvpn-blacklist 0.4 list of blacklisted OpenVPN RSA shared keys
ii opera 11.60.1185 Fast and secure web browser and Internet suite
ii ophcrack 3.3.0-1 Microsoft Windows password cracker using rainbow tables (gui)
ii os-prober 1.38 utility to detect other OSes on a set of drives
ii oscanner 1.0.6-bt2 Oracle assessment framework
ii osvdb 1.0-bt1 Firefox link to osvdb.org.
ii owasp-zap 1.3.4-bt0 An easy to use integrated penetration testing tool for finding vulnerabilities in webapps.
ii oxygen-cursor-theme 0.0.2008-07-07-svn824849-1ubuntu2 Oxygen Mouse Cursor Theme
ii oxygen-icon-theme 4:4.5.3-0ubuntu1~lucid1~ppa1 Oxygen icon theme
ii p0f 2.0.8-bt0 A versatile passive OS fingerprinting tool.
ii p7zip 9.04~dfsg.1-1 7zr file archiver with high compression ratio
ii p7zip-full 9.04~dfsg.1-1 7z and 7za file archivers with high compression ratio
ii pack 0.0.2-bt0 Password Analysis and Cracking Toolkit
ii packagekit 0.5.7-0ubuntu2.2 provides a software installation daemon
ii packagekit-backend-apt 0.5.7-0ubuntu2.2 APT backend for packagekit
ii padbuster 0.3-bt1 PadBuster is a Perl script for automating Padding Oracle Attacks.
ii parted 2.2-5ubuntu5.1 The GNU Parted disk partition resizing program
ii pasco 1.0+20040505-5 An Internet Explorer cache forensic analysis tool
ii passwd 1:4.1.4.2-1ubuntu2.2 change and administer password and group data
ii patch 2.6-2ubuntu1 Apply a diff file to an original
ii pbnj 2.04-bt5 PBNJ is a suite of tools to monitor changes on a network over time. It does this by checking for changes on the target machine(s), which includes the deta
ii pciutils 1:3.0.0-4ubuntu17 Linux PCI Utilities
ii pcmciautils 014-4ubuntu4 PCMCIA utilities for Linux 2.6
ii pcscd 1.5.3-1ubuntu4.2 Middleware to access a smart card using PC/SC (daemon side)
ii pdf-parser 0.3.7-bt1 This tool will parse a PDF document to identify the fundamental elements used in the analyzed file.
ii pdfbook 1.0-bt0 Script to gather facebook artifacts from a pd process memory dump.
ii pdfcrack 0.11-1 PDF files password cracker
ii pdfedit 0.4.3-1 Editor for manipulating PDF documents
ii pdfid 0.0.11-bt0 Will scan a file to look for certain PDF keywords.
ii pdgmail 0.2.0-bt0 Script to gather gmail artifacts from a pd process memory dump.
ii peepdf 0.1-bt1 peepdf is a Python tool to explore PDF files in order to find out if the file can be harmful or not.
ii perl 5.10.1-8ubuntu2.1 Larry Wall's Practical Extraction and Report Language
ii perl-base 5.10.1-8ubuntu2.1 minimal Perl system
ii perl-cisco-copyconfig 1.4-bt2 Provides methods for manipulating the running-config of devices running IOS via SNMP directed TFTP.
ii perl-doc 5.10.1-8ubuntu2.1 Perl documentation
ii perl-modules 5.10.1-8ubuntu2.1 Core Perl modules
ii perl-number-bytes-human 0.07-bt1 Perl module for stuff
ii perl-tk 1:804.028-6 Perl module providing the Tk graphics library
ii perlmagick 7:6.5.7.8-1ubuntu1.1 Perl interface to the ImageMagick graphics routines
ii pgf 2.00-1 TeX Portable Graphic Format
ii phonon 4:4.7.0really4.4.2-0ubuntu1~lucid1~ppa1 metapackage for the Phonon multimedia framework
ii phonon-backend-xine 4:4.7.0really4.4.2-0ubuntu1~lucid1~ppa1 Phonon Xine 1.1.x

backend
ii php5 5.3.2-1ubuntu4.9 server-side, HTML-embedded scripting language (metapackage)
ii php5-cgi 5.3.2-1ubuntu4.9 server-side, HTML-embedded scripting language (CGI binary)
ii php5-cli 5.3.2-1ubuntu4.9 command-line interpreter for the php5 scripting language
ii php5-common 5.3.2-1ubuntu4.9 Common files for packages built from the php5 source
ii php5-gd 5.3.2-1ubuntu4.9 GD module for php5
ii php5-mcrypt 5.3.2-0ubuntu1 MCrypt module for php5
ii php5-mysql 5.3.2-1ubuntu4.9 MySQL module for php5
ii php5-pgsql 5.3.2-1ubuntu4.9 PostgreSQL module for php5
ii php5-sqlite 5.3.2-1ubuntu4.9 SQLite module for php5
ii phpmyadmin 4:3.3.2-1 MySQL web administration tool
ii pidgin 1:2.6.6-1ubuntu4.3 graphical multi-protocol instant messaging client for X
ii pidgin-data 1:2.6.6-1ubuntu4.3 multi-protocol instant messaging client - data files
ii pidgin-guifications 2.16-1 toaster popups for pidgin
ii pidgin-libnotify 0.14-1ubuntu14 display notification bubbles in pidgin
ii pidgin-mbpurple 0.2.4-1ubuntu1 transitional dummy package
ii pidgin-microblog 0.2.4-1ubuntu1 Microblogging plugins for Pidgin
ii pidgin-otr 3.2.0-5 Off-the-Record Messaging plugin for pidgin
ii pidgin-plugin-pack 2.6.2-0ubuntu2 Collection of Pidgin plugins
ii pidgin-skype 20100121+dfsg-1 Skype plugin for libpurple messengers
ii pinentry-gtk2 0.7.6-1 GTK+-2-based PIN or pass-phrase entry dialog for GnuPG
ii pinentry-qt4 0.7.6-1 Qt-4-based PIN or pass-phrase entry dialog for GnuPG
ii pitivi 0.13.4-0ubuntu3 non-linear audio/video editor using GStreamer
ii pkg-config 0.22-1build2 manage compile and link flags for libraries
ii plasma-dataengines-addons 4:4.5.3-0ubuntu1~lucid1~ppa1 addons for KDE 4 Plasma - data engines
ii plasma-dataengines-workspace 4:4.5.3-0ubuntu1~lucid1~ppa1 KDE 4 base workspace Plasma data engines
ii plasma-desktop 4:4.5.3-0ubuntu1~lucid1~ppa1 The KDE Plasma workspace for desktop and laptop computers
ii plasma-runners-addons 4:4.5.3-0ubuntu1~lucid1~ppa1 addons for KDE 4 Plasma - krunner plugins
ii plasma-scriptengine-javascript 4:4.5.3-0ubuntu1~lucid1~ppa1 the JavaScript script engine for Plasma
ii plasma-wallpapers-addons 4:4.5.3-0ubuntu1~lucid1~ppa1 addons for KDE 4 Plasma - wallpaper plugins
ii plasma-widget-folderview 4:4.5.3-0ubuntu1~lucid1~ppa1 Folder View Plasma widget
ii plasma-widget-lancelot 4:4.5.3-0ubuntu1~lucid1~ppa1 addons for KDE 4 Plasma - lancelot widget
ii plasma-widgets-addons 4:4.5.3-0ubuntu1~lucid1~ppa1 addons for KDE 4 Plasma - widgets
ii plasma-widgets-workspace 4:4.5.3-0ubuntu1~lucid1~ppa1 KDE 4 base workspace Plasma widgets and containments
ii plecost 0.2.2-9beta-bt1 Wordpress finger printer tool, plecost search and retrieve information about the plugins versions installed in Wordpress systems.
ii plymouth 0.8.2-2ubuntu2.2 graphical boot animation and logger - main package
ii plymouth-label 0.8.2-2ubuntu2.2 graphical boot animation and logger - label control
ii plymouth-theme-script 0.8.2-2ubuntu2.2 graphical boot animation and logger - script theme

ii plymouth-theme-ubuntu-text 0.8.2-2ubuntu2.2 graphical boot animation and logger - ubuntu-logo theme
ii plymouth-x11 0.8.2-2ubuntu2.2 graphical boot animation and logger - X11 interface
ii pm-utils 1.3.0-1ubuntu3 utilities and scripts for power management
ii pngcrush 1.7.0-1 optimizes PNG (Portable Network Graphics) files
ii pnm2ppa 1.13-0ubuntu1 PPM to PPA converter
ii po-debconf 1.0.16 tool for managing templates file translations with gettext
ii policykit-1 0.96-2ubuntu0.1 framework for managing administrative policies and privileges
ii policykit-1-gnome 0.96-2ubuntu2 GNOME authentication agent for PolicyKit-1
ii polkit-kde-1 0.95.1-2ubuntu1 KDE dialogs for PolicyKit
ii poppler-utils 0.12.4-0ubuntu5.1 PDF utilitites (based on libpoppler)
ii portaudio19-dev 19+svn20090620-0ubuntu2 Portable audio I/O - development files
ii portmap 6.0.0-1ubuntu2.1 RPC port mapper
ii powerfuzzer 1.0beta-bt1 Powerfuzzer is a highly automated and fully customizable web fuzzer (HTTP protocol based application fuzzer).
ii powermgmt-base 1.31 Common utils and configs for power management
ii ppp 2.4.5~git20081126t100229-0ubuntu3 Point-to-Point Protocol (PPP) - daemon
ii pppconfig 2.3.18ubuntu2 A text menu based utility for configuring ppp
ii pppoeconf 1.19ubuntu1 configures PPPoE/ADSL connections
ii pref.pl 1.0-bt0 Parses Prefetch files
ii preview-latex-style 11.85-1ubuntu1 extraction of elements from LaTeX documents as graphics
ii printconf 0.7.9.2+nmu2ubuntu1 automatically configures USB and parallel printers with CUPS
ii privoxy 3.0.15-3 Privacy enhancing HTTP Proxy
ii procps 1:3.2.8-1ubuntu4 /proc file system utilities
ii prosper 1.00.4+cvs.2007.05.01-4 LaTeX class for writing transparencies
ii protos-sip r2-bt1 Evaluate implementation level security and robustness of SIP
ii proxychains 3.1-bt3 a tool that forces any TCP connection made by any given application to follow through proxy like TOR or any other SOCKS4, SOCKS5 or HTTP(S) proxy. Support
ii proxystrike 2.1-bt0 An active Web Application Proxy.
ii proxytunnel 1.9.0-bt3 Connecting outside through HTTP(S) proxies
ii prozilla 2.0.4-1 Package created with checkinstall 1.6.1
ii ps2eps 1.64-6build1 convert PostScript to EPS (Encapsulated PostScript) files
ii psfontmgr 0.11.10-4ubuntu1 PostScript font manager -- part of Defoma, Debian Font Manager
ii psmisc 22.10-1 utilities that use the proc file system
ii psutils 1.17-27 A collection of PostScript document handling utilities
ii ptk 2.0-bt2 PTK forensics is a computer forensic framework for the command line tools in the SleuthKit plus much more software modules.
ii ptunnel 0.71-bt2 Ptunnel is an application that allows you to reliably tunnel TCP connections to a remote host using ICMP echo request and reply packets, commonly known as
ii pure-ftpd 1.0.24-1 Pure-FTPd FTP server
ii pure-ftpd-common 1.0.24-1 Pure-FTPd FTP server (Common Files)
ii putty 0.60+2009-11-22-1 Telnet/SSH client for X
ii putty-tools 0.60+2009-11-22-1 command-line tools for SSH, SCP, and SFTP

ii pwnat 0.3beta-bt4 A tool that allows any number of clients behind NATs to communicate with a server behind a separate NAT.
ii pwntcha rev4780-bt3 PWNtcha stands for "Pretend We re Not a Turing Computer but a Human Antagonist", as well as PWN capTCHAs. This project s goal is to demonstrate the in
ii pyscard 1.6.12-bt1 pyscard is a python module adding smart cards support to python.
ii pyserial 2.5-bt0 Multiplatform Serial Port Module for Python (Win32, Jython, Linux, BSD and more)
ii pytbull 1.3-bt1 Python based Intrusion Detection/Prevention System (IDS/IPS) Testing Framework
ii python 2.6.5-0ubuntu1 An interactive high-level object-oriented language (default version)
ii python-appindicator 0.0.19-0ubuntu4 Python bindings for libappindicator
ii python-apport 1.13.3-0ubuntu2 apport crash report handling library
ii python-apt 0.7.94.2ubuntu6.2 Python interface to libapt-pkg
ii python-beautifulsoup 3.1.0.1-2build1 error-tolerant HTML parser for Python
ii python-cairo 1.8.8-1 Python bindings for the Cairo vector graphics library
ii python-central 0.6.15ubuntu1 register and build utility for Python packages
ii python-chm 0.8.4-1 Python binding for CHMLIB
ii python-clientform 0.2.10-2.1 module for handling HTML forms on the client side
ii python-compizconfig 0.8.2-0ubuntu1 Compiz configuration system bindings
ii python-configobj 4.7.1-1 simple but powerful config file reader and writer for Python
ii python-crypto 2.0.1+dfsg1-4ubuntu2 cryptographic algorithms and protocols for Python
ii python-dbus 0.83.0-1ubuntu3 simple interprocess messaging system (Python interface)
ii python-debian 0.1.14ubuntu2 Python modules to work with Debian-related data formats
ii python-distutils-extra 2.18bzr1 enhancements to the Python build system
ii python-dnspython 1.7.1-1ubuntu0.1 DNS toolkit for Python
ii python-dpkt 1.6+svn54-1 Python packet creation / parsing module
ii python-dumbnet 1.12-3 A dumb, portable networking library -- python bindings
ii python-extractor 1:0.5-7 extracts meta-data from files of arbitrary type (Python bindings)
ii python-flickrapi 1.2-3 Flickr API wrapper for Python
ii python-foomatic 0.7.9.2+nmu2ubuntu1 Python interface to the Foomatic printer database
ii python-fpconst 0.7.2-4 Utilities for handling IEEE 754 floating point special values
ii python-gconf 2.28.0-1ubuntu1 Python bindings for the GConf configuration database system
ii python-gdbm 2.6.5-0ubuntu2 GNU dbm database support for Python
ii python-geoip 1.2.4-2ubuntu1 Python bindings for the GeoIP IP-to-country resolver library
ii python-glade2 2.17.0-0ubuntu2 GTK+ bindings: Glade support
ii python-gnome2 2.28.0-1ubuntu1 Python bindings for the GNOME desktop environment
ii python-gnomecanvas 2.28.0-1ubuntu1 Python bindings for gnomecanvas (debug extension)
ii python-gnupginterface 0.3.2-9.1 Python interface to GnuPG (GPG)
ii python-gnuplot 1.8-1.1 A Python interface to the gnuplot plotting program
ii python-gobject 2.21.1-0ubuntu3 Python bindings for the GObject library
ii python-gst0.10 0.10.18-1 generic media-playing framework (Python bindings)
ii python-gtk2 2.17.0-0ubuntu2 Python bindings for the GTK+ widget set
ii python-gtksourceview2 2.10.1-0ubuntu1 Python bindings for the GtkSourceView widget

ii python-httplib2 0.6.0-1 comprehensive HTTP client library written in Python
ii python-ibus 1.2.0.20091215-1ubuntu4 New input method framework using dbus
ii python-imaging 1.1.7-1ubuntu0.1 Python Imaging Library
ii python-imaging-tk 1.1.7-1ubuntu0.1 Python Imaging Library - ImageTk Module
ii python-impacket 0.9.6.0-3 Python module to easily build and dissect network protocols
ii python-iniparse 0.3.1-1 Module to access and modify configuration data in INI files
ii python-ipy 1:0.70-1 Python module for handling IPv4 and IPv6 addresses and networks
ii python-kde4 4:4.5.3-0ubuntu1~lucid1~ppa5 Python bindings for the KDE 4 libraries
ii python-keybinder 0.0.4-1 register global key bindings for PyGTK-based applications
ii python-launchpad-integration 0.1.35 library for launchpad integration
ii python-launchpadlib 1.6.0-0ubuntu1 Launchpad web services client library
ii python-lazr.restfulclient 0.9.11-1ubuntu1.1 client for lazr.restful-based web services
ii python-lazr.uri 1.0.2-1 library for parsing, manipulating, and generating URIs
ii python-libxml2 2.7.6.dfsg-1ubuntu1.1 Python bindings for the GNOME XML library
ii python-lightblue 0.3.2-1ubuntu1 cross-platform Bluetooth API for Python
ii python-lxml 2.2.4-1 pythonic binding for the libxml2 and libxslt libraries
ii python-magic 5.03-5ubuntu1 File type determination library using "magic" numbers (Python bindings)
ii python-memcache 1.44-1 pure python memcached client
ii python-minimal 2.6.5-0ubuntu1 A minimal subset of the Python language (default version)
ii python-netaddr 0.7.4-1 manipulation of various common network address notations
ii python-newt 0.52.10-5ubuntu1 A NEWT module for Python
ii python-nltk 2.0~b8-0ubuntu1 Python libraries for natural language processing
ii python-notify 0.1.1-2build3 Python bindings for libnotify
ii python-numpy 1:1.3.0-3build1 Numerical Python adds a fast array facility to the Python language
ii python-oauth 1.0a~svn1124-0ubuntu2 implementation of the OAuth protocol
ii python-openssl 0.10-1 Python wrapper around the OpenSSL library
ii python-osmgpsmap 0.7.2-1 GTK+ library to embed OpenStreetMap maps - Python bindings
ii python-packagekit 0.5.7-0ubuntu2.2 PackageKit Python bindings
ii python-pam 0.4.2-12.1ubuntu1 A Python interface to the PAM library
ii python-pcapy 0.10.6-1ubuntu2 Python interface to the libpcap packet capture library
ii python-pefile 1.2.9.1-1 Portable Executable (PE) parsing module for Python
ii python-pexpect 2.3-1build1 Python module for automating interactive applications
ii python-pkg-resources 0.6.10-4ubuntu1 Package Discovery and Resource Access using pkg_resources
ii python-problem-report 1.13.3-0ubuntu2 Python library to handle problem reports
ii python-psyco 1.6-1ubuntu2 Python specializing compiler
ii python-ptrace 0.6.3-bt0 Python binding of ptrace library
ii python-pyasn1 0.0.8a-1 ASN.1 library for Python
ii python-pybonjour 1.1.1-bt4 ybonjour provides a pure-Python interface to Apple Bonjour and compatible DNS-SD libraries (such as Avahi).
ii python-pycurl 7.19.0-3 Python bindings to libcurl
ii python-pydot 1.0.2-1 Python interface to Graphviz's dot
ii python-pyexiv2 0.1.3-6build1 Python binding to Exiv2
ii python-pygoocanvas 0.14.1-0ubuntu1 GooCanvas Python bindings

ii python-pyicu 0.9-2 Python extension wrapping the ICU C++ API
ii python-pymssql 1.0.2+dfsg-1 Python database access for MS SQL server and Sybase
ii python-pyorbit 2.24.0-5ubuntu3 A Python language binding for the ORBit2 CORBA implementation
ii python-pyparsing 1.5.2-1ubuntu1 Python parsing module
ii python-pypcap 1.1.2+debian-2ubuntu1 object-oriented Python interface for libpcap
ii python-pyx 0.10-1ubuntu3 Python module for generating PostScript graphics
ii python-qt3 3.18.1-4ubuntu1 Qt3 bindings for Python
ii python-qt4 4.7.3-1ubuntu2~lucid1~ppa3 Python bindings for Qt4
ii python-qt4-phonon 4.7.3-1ubuntu2~lucid1~ppa3 Python bindings for Phonon
ii python-renderpm 2.4-1 python low level render interface
ii python-reportlab 2.4-1 ReportLab library to create PDF documents using Python
ii python-reportlab-accel 2.4-1 C coded extension accelerator for the ReportLab Toolkit
ii python-scapy 2.0.1-1 Packet generator/sniffer and network scanner/discovery
ii python-scipy 0.7.0-2ubuntu0.1 scientific tools for Python
ii python-serial 2.3-1 pyserial - module encapsulating access for the serial port
ii python-setuptools 0.6.10-4ubuntu1 Python Distutils Enhancements (setuptools compatibility)
ii python-simplejson 2.0.9-1build1 Simple, fast, extensible JSON encoder/decoder for Python
ii python-sip 4.10.2-1ubuntu1~lucid1~ppa1 Python/C++ bindings generator runtime library
ii python-smartpm 1.2-5 Python library of the Smart Package Manager
ii python-soappy 0.12.0-4 SOAP Support for Python
ii python-software-properties 0.75.10.1 manage the repositories that you install software from
ii python-subunit 0.0.5-1 unit testing protocol - Python bindings to generate and consume Subunit streams
ii python-support 1.0.4ubuntu1 automated rebuilding support for Python modules
ii python-svn 1.7.2-2ubuntu1 A(nother) Python interface to Subversion
ii python-testtools 0.9.2-1 Extensions to the Python unittest library
ii python-tk 2.6.5-0ubuntu2 Tkinter - Writing Tk applications with Python
ii python-twisted-bin 10.0.0-2ubuntu2 Event-based framework for internet applications
ii python-twisted-core 10.0.0-2ubuntu2 Event-based framework for internet applications
ii python-twisted-web 10.0.0-1 An HTTP protocol implementation together with clients and servers
ii python-uniconvertor 1.1.4-1build1 Universal vector graphics translator
ii python-uno 1:3.3.2-1ubuntu2~lucid1 Python-UNO bridge
ii python-utidylib 0.2-3.2ubuntu2 Python wrapper for TidyLib
ii python-vte 1:0.23.5-0ubuntu1.1 Python bindings for the VTE widget set
ii python-wadllib 1.1.4-1ubuntu1 Python library for navigating WADL files
ii python-webkit 1.1.7-1 WebKit/Gtk Python bindings
ii python-wicd 1.7.0+ds1-2 wired and wireless network manager - Python module
ii python-wxgtk2.8 2.8.10.1-0ubuntu1.2 wxWidgets Cross-platform C++ GUI toolkit (wxPython binding)
ii python-wxversion 2.8.10.1-0ubuntu1.2 wxWidgets Cross-platform C++ GUI toolkit (wxPython version selector)
ii python-xapian 1.0.17-1ubuntu1 Xapian search engine interface for Python
ii python-xdg 0.18-1ubuntu2 Python library to access freedesktop.org standards

ii python-xlib 0.14+20091101-1 Interface for Python to the X11 Protocol
ii python-yaml 3.09-2build1 YAML parser and emitter for Python
ii python-zope.interface 3.5.3-1ubuntu2 Interfaces for Python
ii python2 2.7.1-bt2 Python 2.7.1
ii python2.6 2.6.5-1ubuntu6 An interactive high-level object-oriented language (version 2.6)
ii python2.6-dev 2.6.5-1ubuntu6 Header files and a static library for Python (v2.6)
ii python2.6-minimal 2.6.5-1ubuntu6 A minimal subset of the Python language (version 2.6)
ii python3 3.1.2-0ubuntu1 An interactive high-level object-oriented language (default python3 version)
ii python3-minimal 3.1.2-0ubuntu1 A minimal subset of the Python language (default python3 version)
ii python3.1 3.1.2-0ubuntu3 An interactive high-level object-oriented language (version 3.1)
ii python3.1-minimal 3.1.2-0ubuntu3 A minimal subset of the Python language (version 3.1)
ii pyxplot 0.7.1+1-1 data plotting program producing publication-quality output
ii qemu 0.12.3+noroms-0ubuntu9.6 dummy transitional pacakge from qemu to qemu-kvm
ii qemu-common 0.12.3+noroms-0ubuntu9.6 qemu common functionality (bios, documentation, etc)
ii qemu-kvm 0.12.3+noroms-0ubuntu9.6 Full virtualization on i386 and amd64 hardware
ii r8187-driver 26.1010.0622.2006-bt0 Patched IEEE r8187 drivers for 2.6.38
ii radeontool 1.6.1-0ubuntu1 utility to control ATI Radeon backlight functions on laptops
ii rainlendar2-lite 2.9.b111-1 Customizable desktop calendar
ii rake 0.8.7-1 a ruby build program
ii rar 1:3.9.b2-1 Archiver for .rar files
ii rarian-compat 0.8.1-4ubuntu1 Documentation meta-data library (compatibility tools)
ii rdate 1:1.2-4build1 sets the system's date from a remote host
ii rdesktop 1.6.0-2ubuntu3 RDP client for Windows NT/2000 Terminal Server
ii rdoc1.8 1.8.7.249-2 Generate documentation from Ruby source files (for Ruby 1.8)
ii rdoc1.9.2 1.9.2.z1-1ppa1~lucid Generate documentation from Ruby source files (for Ruby 1.9.2)
ii readline-common 6.1-1 GNU readline and history libraries, common files
ii readpst 0.6.41-bt0 Utility which can convert email messages to both mbox and MH mailbox formats.
ii reconstructor 2.9 Reconstructor Ubuntu CD Creator
ii recordmydesktop 0.3.8.1+svn602-1ubuntu1 Captures audio-video data of a Linux desktop session
ii recordmydesktop-bt 1.0-bt1 Launcher of RecordMyDesktop for BackTrack Report-Tools.
ii recoverjpeg 2.0-bt0 A tool to recover lost files on damaged memory cards or USB drives.
ii reglookup 0.12.0-bt0 RegLookup is an small command line utility for reading and querying Windows NT-based registries.
ii reiserfsprogs 1:3.6.21-1build1 User-level tools for ReiserFS filesystems
ii revhosts 2.0-bt3 Vhost enumeration and hackign tool
ii rfidiot 1.0a-bt4 RFIDIOt is an open source python library for exploring RFID devices
ii rfuzz 0.9-bt2 RFuzz is a Ruby library to easily test web applications from the outside using a fast HttpClient and wicked evil RandomGenerator allowing the average prog
ii ri 4.2-2~uorppa0 Ruby Interactive reference (ri)
ii ri1.8 1.8.7.249-2 Ruby Interactive reference (for Ruby 1.8)

ii ri1.9.2 1.9.2.z1-1ppa1~lucid Ruby Interactive reference (for Ruby 1.9.2)
ii rifiuti 1.0+20040505-4 A MS Windows recycle bin analysis tool
ii rinetd 0.62-5.1 Internet TCP redirection server
ii rkhunter 1.3.8-bt1 This tool scans for rootkits, backdoors and local exploits.
ii rpm-common 4.7.2-1lbuild1 common files for RPM
ii rrdtool 1.3.8-1ubuntu1 Time-series data storage and display system (programs)
ii rsync 3.0.7-1ubuntu1.1 fast remote file copy program (like rcp)
ii rsyslog 4.2.0-2ubuntu8.1 enhanced multi-threaded syslogd
ii rtpbreak 1.3a-bt2 With rtpbreak you can detect, reconstruct and analyze any RTP session.
ii rtpflood 1.0-bt0 Command line tool used to flood any device processing RTP.
ii rtpinject 1.0-bt1 RTP (Voip) injection tool
ii rtpinsertsound 3.0-bt1 RTP (Voip) securoty tool
ii rtpmixsound 3.0-bt1 RTP (Voip) security tool
ii ruby 4.2-2~uorppa0 An interpreter of object-oriented scripting language Ruby
ii ruby-dev 4.2-2~uorppa0 Header files for compiling extension modules for Ruby
ii ruby1.8 1.8.7.249-2 Interpreter of object-oriented scripting language Ruby 1.8
ii ruby1.8-dev 1.8.7.249-2 Header files for compiling extension modules for the Ruby 1.8
ii ruby1.9.2 1.9.2.z1-1ppa1~lucid Interpreter of object-oriented scripting language Ruby 1.9.2
ii ruby1.9.2-dev 1.9.2.z1-1ppa1~lucid Header files for compiling extension modules for the Ruby 1.9.2
ii rubygems 1.3.7-1~uorppa0 package management framework for Ruby libraries/applications
ii rubygems1.8 1.3.7-1~uorppa0 package management framework for Ruby libraries/applications
ii rubygems1.9.2 1.3.7-1~uorppa0 package management framework for Ruby libraries/applications
ii safecopy 1.6-bt0 A data recovery tool which tries to extract as much data as possible from a problematic source.
ii samba 2:3.4.7~dfsg-1ubuntu3.6 SMB/CIFS file, print, and login server for Unix
ii samba-common 2:3.4.7~dfsg-1ubuntu3.6 common files used by both the Samba server and client
ii samba-common-bin 2:3.4.7~dfsg-1ubuntu3.6 common files used by both the Samba server and client
ii samdump 1.0-bt0 Extracts a Samba-style smbpasswd file directly from an offline copy of the SAM.
ii samdump2 1.1.1-1 Dump Windows 2k/NT/XP password hashes
ii sapyto 0.99-bt0 SAP Penetration Testing Framework
ii sat4j 2.1.1-3 Efficient library of SAT solvers in Java
ii sbd 1.37-bt1 Secure Backdoor Netcat clone
ii scalpel 2.0-bt2 A fast file carver that reads a database of header and footer definitions and extracts matching files or data fragments from a set of image files or raw d
ii scapy 2.2.0-bt0 Scapy is a powerful packet manipulation tool and supports multiple protocols.
ii screen 4.0.3-14ubuntu1.2 terminal multiplexor with VT100/ANSI terminal emulation
ii scrollkeeper 0.8.1-4ubuntu1 Transitional package for scrollkeeper
ii scrot 0.8-11 command line screen capture utility

ii scrounge-ntfs 0.9-bt0 A data recovery program for NTFS filesystems.
ii sctpscan 12.0-bt2 SCTPscan can scan networks for SCTP aware machines and open ports.
ii seabios 0.5.1-0ubuntu2 legacy BIOS implementation which can be used as a coreboot payload
ii securityfocus 1.0-bt1 Firefox link to SecurityFocus.com.
ii sed 4.2.1-6 The GNU sed stream editor
ii sendemail 1.56-1 lightweight, command line SMTP email client
ii sensible-utils 0.0.1ubuntu3 Utilities for sensible alternative selection
ii set 2.5.3-bt0 The Social-Engineer Toolkit (SET) is an open source, python driven tool for penetration testers.
ii sfuzz 0.7.0alpha-bt2 simple fuzz is exactly what it sounds like - a simple fuzzer. don't mistake simple with a lack of fuzz capability. this fuzzer has two network modes of op
ii sgml-base 1.26 SGML infrastructure and SGML catalog file support
ii sgml-data 2.0.4 common SGML and XML data
ii shared-desktop-ontologies 0.5-0ubuntu1~lucid1~ppa1 shared ontologies for semantic searching
ii shared-mime-info 0.71-1ubuntu2 FreeDesktop.org shared MIME database and spec
ii sharutils 1:4.6.3-4 shar, unshar, uuencode, uudecode
ii shodan 1.0-bt2 Firefox link to ShodanHQ.com.
ii sickfuzz 1.0-bt0 sickfuzz is a fuzzer made out of several custom .spk files and a python script to wrap them up, including some tshark support and other features.
ii sidguesser 1.0.5-bt2 Guesses sids/instances against an Oracle database
ii sidplay-base 1.0.9-6 Music player for tunes from C64 and C128 (console)
ii siege 2.70-bt1 Siege is an http load testing and benchmarking utility.
ii simple-ccsm 0.8.2-0ubuntu1 Simple Compizconfig settings manager
ii sipcrack 0.3-bt2 SIPcrack is a suite for sniffing and cracking the digest authentification used in the SIP protocol
ii sipp 3.2-bt0 SIPp is a free Open Source test tool, traffic generator for the SIP protocol
ii sipsak 0.9.6-bt0 A small command line tool for developers and administrators of Session Initiation Protocol (SIP) applications.
ii sipscan 0.1-bt1 A fast network scanner for UDP-SIP clients.
ii sipvicious 0.2.6-bt0 SIPVicious suite is a set of tools that can be used to audit SIP based VoIP systems.
ii skipfish 2.03-bt0 A fully automated, active web application security reconnaissance tool.
ii skype 2.2.0.35-1 Skype
ii sl 3.03-16 Correct you if you type `sl' by mistake
ii sleuthkit 3.2.1-bt0 The Sleuth Kit (TSK) is a C library and a collection of command line tools. Autopsy is a graphical interface to TSK. TSK can be integrated into automated
ii smap 0.6.0-bt0 A simple scanner for SIP enabled devices.
ii smartdimmer 0.8b4-1ubuntu3 Change LCD brightness on Geforce cards
ii smbclient 2:3.4.7~dfsg-1ubuntu3.6 command-line SMB/CIFS clients for Unix
ii smbfs 2:3.4.7~dfsg-1ubuntu3.6 Samba file system utilities
ii smistrip 0.4.8+dfsg2-2 extract MIB from text files like RFC
ii smplayer 0.6.8-2 complete front-end for MPlayer
ii smplayer-themes 0.1.20+dfsg-1 complete front-end for MPlayer - icon themes
ii smplayer-translations 0.6.8-2 complete front-end for MPlayer - translation files
ii smtp-user-enum 1.2-bt0 Username guessing tool primarily for use against the default Solaris SMTP service

ii smtprc 2.0.3-bt0 A network open mail relay checker.
ii smtpscan 0.5-bt0 A tool to guess which MTA is used by sending several "special" SMTP requests.
ii sniffjoke 0.4.1-bt1 SniffJoke is an application for Linux that handle transparently your TCP connection, delaying, modifyng and inject fake packets inside your transmission,
ii snmp 5.4.2.1~dfsg0ubuntu1-0ubuntu2.1 SNMP (Simple Network Management Protocol) applications
ii snmp-mibs-downloader 1.0 Install and manage Management Information Base (MIB) files
ii snmpcheck 1.8-bt2 Like to snmpwalk, snmpcheck permits to enumerate information via SNMP protocol.
ii snmpenum 1.0-bt2 Simple Perl script to enumerate information on Machines that are running SNMP
ii snort 2.8.5.2-2build1 flexible Network Intrusion Detection System
ii snort-common 2.8.5.2-2build1 flexible Network Intrusion Detection System [common files]
ii snort-common-libraries 2.8.5.2-2build1 flexible Network Intrusion Detection System ruleset
ii snort-rules-default 2.8.5.2-2build1 flexible Network Intrusion Detection System ruleset
ii socat 1.7.1.3-bt2 socat is a relay for bidirectional data transfer between two independent data channels. Each of these data channels may be a file, pipe, device (serial li
ii software-properties-gtk 0.75.10.1 manage the repositories that you install software from
ii software-properties-kde 0.75.10.1 manage the repositories that you install software from
ii soprano-daemon 2.5.0+dfsg.1-1ubuntu1~lucid1~ppa2 daemon for the Soprano RDF framework
ii sox 14.3.0-1.1build1 Swiss army knife of sound processing
ii spamhole 0.4-bt0 spamhole is a fake sopen SMTP relay, intended to stop (some) spam by convincing spammers that it is delivering spam messages for them, when in fact it is
ii spike 2.9-bt5 A powerful network fuzzer.
ii sqlbrute 1.0-bt3 Multi-threaded blind SQL injection bruteforcer.
ii sqldict 2.1-bt0 SQLdict is a dictionary attack tool for SQL Server.
ii sqlfairy 0.11003-1 SQL translation utilities
ii sqlite 2.8.17-6build2 command line interface for SQLite
ii sqlite3 3.6.22-1 A command line interface for SQLite 3
ii sqllhf 3.2-bt0 SQL Server Brute Forcing tool featuring a scriptable command-line interface.
ii sqlmap 0.9-bt2 sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of back-end d
ii sqlninja 0.2.6-bt1 Sqlninja is a tool targeted to exploit SQL Injection vulnerabilities on a web application that uses Microsoft SQL Server.
ii sqlscan 1.0-bt0 SQL Scanner that will collect hosts using a google query.
ii squashfs-tools 1:4.0-6ubuntu1 Tool to create and append to squashfs filesystems
ii ssh-askpass-gnome 1:5.3p1-3ubuntu6 interactive X program to prompt users for a passphrase for ssh-add
ii ssidsniff 0.53-bt2 A curses based tool that allows identification, classification and data capturing of wireless networks. The interface is inspired by the unix top(1) utili
ii ssl-cert 1.0.23ubuntu2 simple debconf wrapper for OpenSSL
ii ssldump 0.9b3-bt0 An SSLv3/TLS network protocol analyzer.

ii sslh 1.8rc4-bt0 Lets one accept both HTTPS and SSH connections on the same port.
ii sslscan 1.8.2-bt2 SSLScan determines what ciphers are supported on SSL-based services, such as HTTPS. Furthermore, SSLScan will determine the prefered ciphers of the SSL se
ii sslsniff 0.8-bt0 Designed to MITM all SSL connections on a LAN and dynamically generate certs.
ii sslstrip 0.9-bt0 Transparently hijacks HTTP traffic on a network.
ii stegdetect 0.6-bt0 Stegdetect is an automated tool for detecting steganographic content in images. It is capable of detecting several different steganographic methods to emb
ii stopwatch 3.5-2 A virtual stopwatch and timer
ii strace 4.5.19-2 A system call tracer
ii streamripper 1.64.6-1 download online streams into audio files
ii stunnel4 4.35-bt2 The stunnel program is designed to work as an SSL encryption wrapper between remote client and local (inetd-startable) or remote servers. The goal is to f
ii subversion 1.6.6dfsg-2ubuntu1.2 Advanced version control system
ii sudo 1.7.2p1-1ubuntu5.3 Provide limited super user privileges to specific users
ii swaks 20100211-bt0 A flexible, scriptable, transaction-oriented SMTP test tool.
ii swh-plugins 0.4.15+1-4 Steve Harris's LADSPA plugins
ii swig 1.3.40-2ubuntu1 Generate scripting interfaces to C/C++ code
ii synaptic 0.63.1ubuntu7 Graphical package manager
ii syslinux 2:3.63+dfsg-2ubuntu3 Bootloader for Linux/i386 using MS-DOS floppies
ii systemsettings 4:4.5.3-0ubuntu1~lucid1~ppa1 KDE 4 System Settings
ii sysv-rc 2.87dsf-4ubuntu17.2 System-V-like runlevel change mechanism
ii sysvinit-utils 2.87dsf-4ubuntu17.2 System-V-like utilities
ii t50 5.4.0-bt0 Experimental packet injector tool.
ii tar 1.22-2ubuntu1 GNU version of the tar archiving utility
ii tasksel 2.73ubuntu26 Tool for selecting tasks for installation on Debian systems
ii tasksel-data 2.73ubuntu26 Official tasks used for installation of Debian systems
ii tcl 8.4.16-2 The Tool Command Language (default version) - run-time files
ii tcl-dev 8.4.16-2 The Tool Command Language (default version) - development files
ii tcl-doc 8.4.16-2 The Tool Command Language (default version) - manual pages
ii tcl8.4 8.4.19-4 Tcl (the Tool Command Language) v8.4 - run-time files
ii tcl8.4-dev 8.4.19-4 Tcl (the Tool Command Language) v8.4 - development files
ii tcl8.4-doc 8.4.19-4 Tcl (the Tool Command Language) v8.4 - manual pages
ii tcl8.5 8.5.8-2 Tcl (the Tool Command Language) v8.5 - run-time files
ii tclreadline 2.1.0-10 GNU Readline Extension for Tcl/Tk
ii tcpd 7.6.q-18 Wietse Venema's TCP wrapper utilities
ii tcpdump 4.1.1-bt6 A powerful command-line packet analyzer.
ii tcpflow 0.21.ds1-6 TCP flow recorder
ii tcpreplay 3.4.4-bt1 Tcpreplay is a suite written by Aaron Turner for UNIX operating systems which gives you the ability to use previously captured traffic in libpcap format
ii tcptraceroute 1.5beta7-bt3 tcptraceroute is a traceroute implementation using TCP packets.
ii tcptrack 1.4.0-0ubuntu0.1~lucid TCP connection tracker, with states and speeds
ii tcpxtract 1.0.1-5 extracts files from network traffic based on file signatures
ii teamviewer6 6.0.9258 TeamViewer (Remote Control Application)
ii telnet 0.17-36build1 The telnet client
ii terminator 0.93-0ubuntu1 multiple GNOME terminals in one window
ii testdisk 6.11.3-bt0 Powerful free data recovery software.

ii testssl.sh 1.13-bt1 testssl.sh is a Unix command line tool which checks for the support of weak and medium (i.e. also weak) SSL ciphers and the old SSL version 2.
ii tex-common 2.06ubuntu0.1 common infrastructure for building and installing TeX
ii texlive 2009-7 TeX Live: A decent selection of the TeX Live packages
ii texlive-base 2009-7 TeX Live: Essential programs and files
ii texlive-binaries 2009-5ubuntu0.2 Binaries for TeX Live
ii texlive-common 2009-7 TeX Live: Base component
ii texlive-doc-base 2009-2 TeX Live: TeX Live documentation
ii texlive-extra-utils 2009-7ubuntu3 TeX Live: TeX auxiliary programs
ii texlive-font-utils 2009-7ubuntu3 TeX Live: TeX and Outline font utilities
ii texlive-fonts-recommended 2009-7 TeX Live: Recommended fonts
ii texlive-fonts-recommended-doc 2009-7 TeX Live: Documentation files for texlive-fonts-recommended
ii texlive-generic-recommended 2009-7 TeX Live: Recommended generic packages
ii texlive-latex-base 2009-7 TeX Live: Basic LaTeX packages
ii texlive-latex-base-doc 2009-7 TeX Live: Documentation files for texlive-latex-base
ii texlive-latex-extra 2009-7ubuntu3 TeX Live: LaTeX supplementary packages
ii texlive-latex-extra-doc 2009-7ubuntu3 TeX Live: Documentation files for texlive-latex-extra
ii texlive-latex-recommended 2009-7 TeX Live: LaTeX recommended packages
ii texlive-luatex 2009-7 TeX Live: LuaTeX packages
ii texlive-pictures 2009-7 TeX Live: Graphics packages and programs
ii texlive-pstricks 2009-7ubuntu3 TeX Live: PSTricks packages
ii tftpbruteforce 0.1-bt1 TFTP filename bruteforcer
ii thc-ipv6 1.8-bt0 A complete tool set to attack the inherent protocol weaknesses of IPV6.
ii thc-pptp-bruter 0.1.4-bt0 Brute force program against pptp vpn endpoints (tcp port 1723).
ii thcsslcheck 0.1-bt2 Windows tool that checks the remote ssl stack for supported ciphers and version.
ii theharvester 2.1-bt0 theHarvester is a tool for gathering e-mail accounts and subdomain names from different public sources.
ii thunar-data 1.0.1-3ubuntu1 Provides thunar documentation, icons and translations
ii thunderbird 3.1.10+build1+nobinonly-0ubuntu0.10.04.1 mail/news client with RSS and integrated spam filter support
ii time 1.7-23build1 The GNU time program for measuring cpu resource usage
ii tinyproxy 1.8.2-bt1 Tinyproxy is a light-weight HTTP proxy daemon for POSIX operating systems. Designed from the ground up to be fast and yet small, it is an ideal solution f
ii tk 8.4.16-2 The Tk toolkit for Tcl and X11 (default version) - run-time files
ii tk-dev 8.4.16-2 The Tk toolkit for Tcl and X11 (default version) - development files
ii tk-doc 8.4.16-2 The Tk toolkit for Tcl and X11 (default version) - manual pages
ii tk8.4 8.4.19-4 Tk toolkit for Tcl and X11, v8.4 - run-time files
ii tk8.4-dev 8.4.19-4 Tk toolkit for Tcl and X11, v8.4 - development files
ii tk8.4-doc 8.4.19-4 Tk toolkit for Tcl and X11, v8.4 - manual pages
ii tk8.5 8.5.8-1 Tk toolkit for Tcl and X11, v8.5 - run-time files
ii tlssled 1.1-bt0 Shell script whose purpose is to evaluate the security of a target SSL/TLS implementation
ii tofrodos 1.7.8.debian.1-2 Converts DOS <-> Unix text files, alias tofromdos
ii tor 0.2.2.35-1~lucid+1 anonymizing overlay network for TCP

ii tor-geoipdb 0.2.2.35-1~lucid+1 geoIP database for Tor
ii torsocks 1.0~epsilon+dfsg1-1 use socks-friendly applications with Tor
ii traceroute 2.0.13-bt2 This is a new modern implementation of traceroute(8) utility for Linux systems.
ii transfig 1:3.2.5.a-2.1 Utilities for converting XFig figure files
ii truecrypt 7.0-bt4 open-source disk encryption software
ii tsconf 1.0-7build1 touch screen library common files
ii ttf-arabeyes 2.0-5 Arabeyes GPL TrueType Arabic fonts
ii ttf-dejavu 2.30-2 Metapackage to pull in ttf-dejavu-core and ttf-dejavu-extra
ii ttf-dejavu-core 2.30-2 Vera font family derivate with additional characters
ii ttf-dejavu-extra 2.30-2 Vera font family derivate with additional characters
ii ttf-droid 1.00~b112+dfsg+1-0ubuntu1 handheld device font with extensive style and language support
ii ttf-dustin 20030517-7 Various TrueType fonts from dustismo.com
ii ttf-freefont 20090104-5 Freefont Serif, Sans and Mono Truetype fonts
ii ttf-kacst 2.0+mry-2ubuntu1 KACST free TrueType Arabic fonts
ii ttf-kacst-one 3.0-1ubuntu2 TrueType font designed for Arabic language
ii ttf-liberation 1.05.2.20091019-4 Fonts with the same metrics as Times, Arial and Courier
ii ttf-mscorefonts-installer 3.2ubuntu0.1 Installer for Microsoft TrueType core fonts
ii ttf-opensymbol 2:2.4.3+LibO3.3.2-1ubuntu2~lucid1 OpenSymbol TrueType font
ii ttf-sil-gentium 20081126:1.02-10 extended Unicode Latin font ("a typeface for the nations")
ii ttf-sil-gentium-basic 1.1-2 smart Unicode font families (Basic and Book Basic) based on Gentium
ii ttf-symbol-replacement 1.2.2-0ubuntu2~lucid1 Free font with the same metrics as Symbol
ii ttf-takao-gothic 003.02.01-2ubuntu1 Japanese TrueType font set, Takao Gothic Fonts
ii ttf-takao-mincho 003.02.01-2ubuntu1 Japanese TrueType font set, Takao Mincho Fonts
ii ttf-takao-pgothic 003.02.01-2ubuntu1 Japanese TrueType font set, Takao P Gothic Font
ii ttf-ubuntu-font-family 0.70.1-0ubuntu1~lucid2 Ubuntu Font Family, sans-serif typeface hinted for clarity
ii ttf-umefont 411-1 Japanese TrueType font, Ume-font
ii ttf-unfonts-core 1.0.1-7ubuntu1 Un series Korean TrueType fonts
ii tuxcut 3.2 TuxCut
ii twolame 0.3.12-1 MPEG Audio Layer 2 encoder (command line frontend)
ii tzdata 2011g-0ubuntu0.10.04 time zone and daylight-saving time data
ii tzdata-java 2011g-0ubuntu0.10.04 time zone and daylight-saving time data for use by java runtimes
ii ua-tester 1.06-bt2 his tool is designed to automatically check a given URL using a list of standard and non-standard User Agent strings provided by the user (1 per line).
ii ubuntu-keyring 2010.11.09 GnuPG keys of the Ubuntu archive
ii ubuntu-serverguide 10.04.3 The Ubuntu Server Guide
ii ucf 3.0025 Update Configuration File: preserve user changes to config files.
ii uck 2.0.12-0ubuntu2 Tool to customize official Ubuntu Live CDs
ii udev 151-12.3 rule-based device node and kernel event manager
ii udisks 1.0.1-1ubuntu1 abstraction for enumerating block devices
ii udp.pl 1.0-bt2 UDP flooder.
ii udptunnel r16-bt2 Tunnels TCP over UDP packets.

ii ufraw 0.16-1build1 standalone importer for raw camera images
ii ufw 0.30pre1-0ubuntu2 program for managing a Netfilter firewall
ii unace 1.2b-7 extract, test and view .ace archives
ii unattended-upgrades 0.55ubuntu6 automatic installation of security upgrades
ii unetbootin-bt 1.0-bt0 UNetbootin allows you to create bootable Live USB drives for Ubuntu, Fedora, and other Linux distributions without burning a CD.
ii unhide 20080519-6 Forensic tool to find hidden processes and ports
ii unicornscan 0.4.7-bt9 Unicornscan is a new information gathering and correlation engine built for and by members of the security research and testing communities.
ii uniscan 5.2-bt0 An open source vulnerability scanner for Web applications.
ii uno-libs3 1.7.0+LibO3.3.2-1ubuntu2~lucid1 LibreOffice UNO runtime environment -- public shared libraries
ii unrar 1:3.9.3-1 Unarchiver for .rar files (non-free version)
ii unrar-free 1:0.0.1+cvs20071127-1 Unarchiver for .rar files
ii untidy beta2-bt1 untidy is general purpose XML Fuzzer.
ii unzip 6.0-1build1 De-archiver for .zip files
ii update-inetd 4.35ubuntu0.1 inetd configuration file updater
ii update-manager 1:0.134.11 GNOME application that manages apt updates
ii update-manager-core 1:0.134.11 manage release upgrades
ii update-manager-kde 1:0.134.11 Support modules for Update Notifier KDE
ii update-notifier-common 0.99.3 Files shared between update-notifier and adept
ii upstart 0.6.5-8 event-based init daemon
ii ure 1.7.0+LibO3.3.2-1ubuntu2~lucid1 LibreOffice UNO runtime environment
ii ureadahead 0.100.0-4.1.3 Read required files in advance
ii usb-modeswitch 1.1.0-2 mode switching tool for controlling "flip flop" USB devices
ii usb-modeswitch-data 20100127-1 mode switching data for usb-modeswitch
ii usbmuxd 1.0.2-1ubuntu2 USB multiplexor daemon for iPhone and iPod Touch devices
ii usbutils 0.86-2ubuntu1 Linux USB utilities
ii user-setup 1.28ubuntu7 Set up initial user and password
ii util-linux 2.17.2-0ubuntu1.10.04.2 Miscellaneous system utilities
ii uuid 1.6.2-1ubuntu1 the Universally Unique Identifier Command-Line Tool
ii uuid-runtime 2.17.2-0ubuntu1.10.04.2 runtime components for the Universally Unique ID library
ii v86d 0.1.9-1ubuntu1 daemon to run x86 code in an emulated environment
ii vbetool 1.1-2 run real-mode video BIOS code to alter hardware state
ii vega 1.0-bt0 An open source platform to test the security of web applications.
ii vgabios 0.6c-2ubuntu1 VGA BIOS software for the Bochs and Qemu emulated VGA card
ii videocut 0.2.0-5 application for creating compositions of screenshots from videos
ii videojak 2.00-bt3 VideoJak is an IP Video security assessment tool that can simulate a proof of concept video interception or replay test.
ii vim 2:7.2.330-1ubuntu3 Vi IMproved - enhanced vi editor
ii vim-common 2:7.2.330-1ubuntu3 Vi IMproved - Common files
ii vim-runtime 2:7.2.330-1ubuntu3 Vi IMproved - Runtime files
ii vim-tiny 2:7.2.330-1ubuntu3 Vi IMproved - enhanced vi editor - compact version
ii vinetto 0.7-bt2 Vinetto is a forensics tool to examine Thumbs.db files.
ii virtuoso-minimal 6.1.2+dfsg1-1ubuntu4~lucid1~ppa1 high-performance database - core dependency package
ii virtuoso-opensource-6.1-bin 6.1.2+dfsg1-1ubuntu4~lucid1~ppa1 high-performance

database - binaries
ii virtuoso-opensource-6.1-common 6.1.2+dfsg1-1ubuntu4~lucid1~ppa1 high-performance database - common files
ii vlan 1.9-3ubuntu3 user mode programs to enable VLANs on your ethernet devices
ii vlc 1.0.6-1ubuntu1.6 multimedia player and streamer
ii vlc-data 1.0.6-1ubuntu1.6 Common data for VLC
ii vlc-nox 1.0.6-1ubuntu1.6 multimedia player and streamer (without X support)
ii vlc-plugin-pulse 1.0.6-1ubuntu1.6 PulseAudio plugin for VLC
ii voiper 0.07-bt3 VoIPER is a security toolkit that aims to allow developers and security researchers to easily, extensively and automatically test VoIP devices for securit
ii voiphopper 1.0-bt0 VoIP Hopper is a GPLv3 licensed security tool, written in C, that rapidly runs a VLAN Hop into the Voice VLAN on specific Ethernet switches. VoIP Hopper d
ii voipong 2.0-bt1 utility which detects all Voice Over IP calls on a pipeline
ii volafox 0.6-bt0 Memory Analyzer for Mac OS X
ii volatility 2.0-bt1 A completely open collection of tools, implemented in Python under the GNU General Public License, for the extraction of digital artifacts from volatile m
ii w3af 1.1-bt1 w3af is a Web Application Attack and Audit Framework. The project's goal is to create a framework to find and exploit web application vulnerabilities that
ii w3m 0.5.2-2.1ubuntu1.2 WWW browsable pager with excellent tables/frames support
ii waffit 0.9.0-bt1 WAFW00F allows one to identify and fingerprint WAF products protecting a website.
ii wamerican 6-3 American English dictionary words for /usr/share/dict
ii wapiti 2.2.1-bt2 Web application vulnerability scanner, & security auditor.
ii warvox 1.0.1-bt1 WarVOX is a suite of tools for exploring, classifying, and auditing telephone systems.
ii wbar 1.3.3+dfsg2-1 light and fast launch bar
ii wbarconf 0.7.2-bt2 wbar configuration gui written with Python and GTK.
ii wbritish 6-3 British English dictionary words for /usr/share/dict
ii webscarab 1.0-bt0 WebScarab operates as a HTTP and HTTPS intercepting proxy, allowing the operator to review and modify requests and responses.
ii websecurify 0.9-bt0 Websecurify is a powerful web application security testing environment designed from the ground up to provide the best combination of automatic and manual
ii webshag 1.10-bt3 Webshag is a multi-threaded, multi-platform web server audit tool. Written in Python, it gathers commonly useful functionalities for web server auditing l
ii webshells 1.0-bt3 collection of web shell
ii webslayer rev5-bt0 A tool designed for bruteforcing Web Applications.
ii weevely 0.3-bt0 Weevely generate PHP code to trojanize a web server, and act like a client to estabilish a telnet-like connection or inject addictional function on backdo
ii wepcrack 0.1-bt2 WEPCrack is an open source tool for breaking 802.11 WEP secret keys.
ii wfuzz 2.0-bt0 Wfuzz is a tool designed for bruteforcing Web Applications, it can be used for finding resources not linked (directories, servlets, scripts, etc), brutefo
ii wget 1.12-1.1ubuntu2.1 retrieves files from the web
ii whatweb 0.4.8-bt0 WhatWeb identifies websites.
ii whiptail 0.52.10-5ubuntu1 Displays user-friendly dialog boxes from shell scripts
ii whois 5.0.0ubuntu3 an intelligent whois client
ii wicd 1.7.0+ds1-2 wired and wireless network manager - metapackage
ii wicd-daemon 1.7.0+ds1-2 wired and wireless network manager - daemon

ii wicd-gtk 1.7.0+ds1-2 wired and wireless network manager - GTK+ client
ii wifitap 0.4.0-bt2 WiFi injection tool through tun/tap device
ii winbind 2:3.4.7~dfsg-1ubuntu3.6 Samba nameservice integration server
ii windows-binaries 1.0-bt1 Various windows pentesting binaries.
ii wine 1.2.2-0ubuntu2~lucid1 Microsoft Windows Compatibility Layer (dummy package)
ii wine1.2 1.2.2-0ubuntu2~lucid1 Microsoft Windows Compatibility Layer (Binary Emulator and Library)
ii wine1.2-gecko 1.0.0-0ubuntu4 Microsoft Windows Compatibility Layer (Web Browser)
ii winff 1.2.0-1ubuntu2 graphical video and audio batch converter using ffmpeg
ii winff-doc 1.2.0-1ubuntu2 winff documentation
ii wireless-crda 1.12 Wireless Central Regulatory Domain Agent
ii wireless-tools 30~pre9-3ubuntu4 Tools for manipulating Linux Wireless Extensions
ii wireshark 1.6.4-bt0 A network "sniffer" - a tool that captures and analyzes packets off the wire.
ii wmctrl 1.07-6 control an EWMH/NetWM compatible X Window Manager
ii wodim 9:1.1.10-1ubuntu1 command line CD/DVD writing tool
ii wordlists 1.0-bt0 wordlists
ii wpasupplicant 0.6.9-3ubuntu3 client support for WPA and WPA2 (IEEE 802.11i)
ii wpscan 1.1-bt2 A vulnerability scanner which checks the security of WordPress installations.
ii wstool 0.14001-bt4 WSTOOL is OS-independence Web vulnerable scanner.
ii wvdial 1.60.3 PPP dialer with built-in intelligence
ii wwwconfig-common 0.2.1 Debian web auto configuration
ii x-ttcidfont-conf 32 TrueType and CID fonts configuration for X
ii x11-apps 7.5+1ubuntu2 X applications
ii x11-common 1:7.5+5ubuntu1 X Window System (X.Org) infrastructure
ii x11-session-utils 7.5+1 X session utilities
ii x11-utils 7.5+3 X11 utilities
ii x11-xfs-utils 7.4+1build2 X font server utilities
ii x11-xkb-utils 7.5+1 X11 XKB utilities
ii x11-xserver-utils 7.5+1ubuntu2.1 X server utilities
ii x11proto-composite-dev 1:0.4.1-1 X11 Composite extension wire protocol
ii x11proto-core-dev 7.0.16-1 X11 core wire protocol and auxiliary headers
ii x11proto-damage-dev 1:1.2.0-1 X11 Damage extension wire protocol
ii x11proto-fixes-dev 1:4.1.1-2 X11 Fixes extension wire protocol
ii x11proto-input-dev 2.0-2 X11 Input extension wire protocol
ii x11proto-kb-dev 1.0.4-1 X11 XKB extension wire protocol
ii x11proto-randr-dev 1.3.1-1 X11 RandR extension wire protocol
ii x11proto-render-dev 2:0.11-1 X11 Render extension wire protocol
ii x11proto-xext-dev 7.1.1-2 X11 various extension wire protocol
ii x11proto-xinerama-dev 1.2-2 X11 Xinerama extension wire protocol
ii xauth 1:1.0.4-1 X authentication utility
ii xbase-clients 1:7.5+5ubuntu1 miscellaneous X clients - metapackage
ii xbitmaps 1.1.0-1 Base X bitmaps
ii xchat 2.8.6-4ubuntu5 IRC client for X similar to AmIRC
ii xchat-common 2.8.6-4ubuntu5 Common files for X-Chat
ii xchm 2:1.17-2 Compiled HTML Help (CHM) file viewer for X
ii xdg-user-dirs 0.12-0ubuntu2 tool to manage well known user directories

ii xdg-utils 1.0.2-6.1ubuntu3.1 desktop integration utilities from freedesktop.org
ii xdotool 20090330-1 simulate X11 keyboard/mouse input
ii xfburn 0.4.3-1 CD-burner application for Xfce Desktop Environment
ii xfce-keyboard-shortcuts 4.6.3-2 xfce keyboard shortcuts configuration
ii xfconf 4.6.1-2ubuntu2 utilities for managing settings in Xfce
ii xfonts-base 1:1.0.1 standard fonts for X
ii xfonts-encodings 1:1.0.3-1 Encodings for X.Org fonts
ii xfonts-mathml 4ubuntu1 Type1 Symbol font for MathML
ii xfonts-utils 1:7.5+2 X Window System font utility programs
ii xgps 1.1.5-bt0 xGPS is a free project aiming to bring powerful and easy to use navigation software
ii xine-ui 0.99.5+cvs20070914-2.1 the xine video player, user interface
ii xinit 1.2.0-1 X server initialisation tool
ii xkb-data 1.8-1ubuntu8.1~10.04.1 X Keyboard Extension (XKB) configuration data
ii xml-core 0.13 XML infrastructure and XML catalog file support
ii xmltoman 0.4-2 simple XML to man converter
ii xpdf-common 3.02-2ubuntu1.1 Portable Document Format (PDF) suite -- common files
ii xpdf-reader 3.02-2ubuntu1.1 Portable Document Format (PDF) suite -- viewer for X11
ii xplico 0.7.0-bt0 The goal of Xplico is extract from an internet traffic capture the applications data contained.
ii xpp 1.5-cvs20050828-1ubuntu3 X Printing Panel
ii xprobe2 2.1-bt2 Active OS fingerprinting tool.
ii xresprobe 0.4.24ubuntu9 X Resolution Probe
ii xsensors 0.70-1ubuntu1 A hardware health information viewer
ii xserver-common 2:1.7.6-2ubuntu7.6 common files used by various X servers
ii xserver-xephyr 2:1.7.6-2ubuntu7.6 nested X server
ii xserver-xorg 1:7.5+5ubuntu1 the X.Org X server
ii xserver-xorg-core 2:1.7.6-2ubuntu7.6 Xorg X server - core server
ii xserver-xorg-input-all 1:7.5+5ubuntu1 the X.Org X server -- input driver metapackage
ii xserver-xorg-input-evdev 1:2.3.2-5ubuntu1 X.Org X server -- evdev input driver
ii xserver-xorg-input-mouse 1:1.5.0-1 X.Org X server -- mouse input driver
ii xserver-xorg-input-synaptics 1.2.2-1ubuntu4 Synaptics TouchPad driver for X.Org server
ii xserver-xorg-input-vmmouse 1:12.6.5-4ubuntu2 X.Org X server -- VMMouse input driver to use with VMWare
ii xserver-xorg-input-wacom 1:0.10.5-0ubuntu4.1 X.Org X server -- Wacom input driver
ii xserver-xorg-video-all 1:7.5+5ubuntu1 the X.Org X server -- output driver metapackage
ii xserver-xorg-video-apm 1:1.2.2-1 X.Org X server -- APM display driver
ii xserver-xorg-video-ark 1:0.7.2-1 X.Org X server -- ark display driver
ii xserver-xorg-video-ati 1:6.13.0-1ubuntu5 X.Org X server -- AMD/ATI display driver wrapper
ii xserver-xorg-video-chips 1:1.2.2-1 X.Org X server -- Chips display driver
ii xserver-xorg-video-cirrus 1:1.3.2-1ubuntu1 X.Org X server -- Cirrus display driver
ii xserver-xorg-video-fbdev 1:0.4.1-1ubuntu1 X.Org X server -- fbdev display driver
ii xserver-xorg-video-geode 2.11.11-1~lucid1 X.Org X server -- Geode GX2/LX display driver
ii xserver-xorg-video-i128 1:1.3.3-1 X.Org X server -- i128 display driver
ii xserver-xorg-video-i740 1:1.3.2-1 X.Org X server -- i740 display driver
ii xserver-xorg-video-intel 2:2.9.1-3ubuntu5 X.Org X server -- Intel i8xx, i9xx display driver
ii xserver-xorg-video-mach64 6.8.2-2 X.Org X server -- ATI Mach64 display driver

ii xserver-xorg-video-mga 1:1.4.11.dfsg-2ubuntu1 X.Org X server -- MGA display driver
ii xserver-xorg-video-neomagic 1:1.2.4-2 X.Org X server -- Neomagic display driver
ii xserver-xorg-video-nouveau 1:0.0.15+git20100219+9b4118d-0ubuntu5 X.Org X server -- Nouveau display driver (experimental)
ii xserver-xorg-video-nv 1:2.1.15-1ubuntu3 X.Org X server -- NV display driver
ii xserver-xorg-video-openchrome 1:0.2.904+svn827-1 X.Org X server -- VIA display driver
ii xserver-xorg-video-r128 6.8.1-2ubuntu1 X.Org X server -- ATI r128 display driver
ii xserver-xorg-video-radeon 1:6.13.0-1ubuntu5 X.Org X server -- AMD/ATI Radeon display driver
ii xserver-xorg-video-rendition 1:4.2.3-1 X.Org X server -- Rendition display driver
ii xserver-xorg-video-s3 1:0.6.3-1 X.Org X server -- legacy S3 display driver
ii xserver-xorg-video-s3virge 1:1.10.4-1 X.Org X server -- S3 ViRGE display driver
ii xserver-xorg-video-savage 1:2.3.1-1ubuntu1 X.Org X server -- Savage display driver
ii xserver-xorg-video-siliconmotion 1:1.7.3-1 X.Org X server -- SiliconMotion display driver
ii xserver-xorg-video-sis 1:0.10.2-2 X.Org X server -- SiS display driver
ii xserver-xorg-video-sisusb 1:0.9.3-1 X.Org X server -- SiS USB display driver
ii xserver-xorg-video-tdfx 1:1.4.3-1 X.Org X server -- tdfx display driver
ii xserver-xorg-video-trident 1:1.3.3-1 X.Org X server -- Trident display driver
ii xserver-xorg-video-tseng 1:1.2.3-1 X.Org X server -- Tseng display driver
ii xserver-xorg-video-v4l 1:0.2.0-4 X.Org X server -- Video 4 Linux display driver
ii xserver-xorg-video-vesa 1:2.3.0-1ubuntu1 X.Org X server -- VESA display driver
ii xserver-xorg-video-vmware 1:10.16.9-1 X.Org X server -- VMware display driver
ii xserver-xorg-video-voodoo 1:1.2.3-1 X.Org X server -- Voodoo display driver
ii xsidplay 2.0.3-1ubuntu1 Music player for tunes from C64
ii xsltproc 1.1.26-1ubuntu1 XSLT command line processor
ii xssed 1.0-bt1 Firefox link to XSSED.com .
ii xsser 1.6-bt0 Cross Site "Scripter" is an automatic -framework- to detect, exploit and report XSS vulnerabilities in web-based aplications.
ii xssfuzz 1.1-bt1 It s for finding new vectors and testing those within the context of multiple encoding methods.
ii xterm 256-1ubuntu1 X terminal emulator
ii xtightvncviewer 1.3.9-6 virtual network computing client software for X
ii xtrans-dev 1.2.5-1 X transport library (development files)
ii xulrunner-1.9.2 1.9.2.17+build3+nobinonly-0ubuntu0.10.04.1 XUL + XPCOM application runner
ii xutils-dev 1:7.5+2 X Window System utility programs for development
ii xvidcap 1.1.7-0.2ubuntu8 Screen video capture for X
ii xz-utils 4.999.9beta+20091116-1 XZ-format compression utilities
ii yakuake 2.9.6-1ubuntu1 a Quake-style terminal emulator based on KDE Konsole technology
ii yelp 2.30.0-0ubuntu2 Help browser for GNOME
ii yersinia 0.7.1-bt0 A network tool designed to take advantage of some weakeness in different network protocols.
ii youtube-dl 2010.04.04-1 download videos from youtube
ii zenity 2.30.0-0ubuntu1 Display graphical dialog boxes from shell scripts
ii zip 3.0-2 Archiver for .zip files
ii zlib1g 1:1.2.3.3.dfsg-15ubuntu1 compression library - runtime
ii zlib1g-dev 1:1.2.3.3.dfsg-15ubuntu1 compression library - development

ii zlibc 0.9k-4.1 An on-fly auto-uncompressing C library
rc apparmor 2.5.1-0ubuntu0.10.04.3 User-space parser utility for AppArmor
rc apparmor-utils 2.5.1-0ubuntu0.10.04.3 Utilities for controlling AppArmor
rc clamtk 4.25-1 graphical front-end for ClamAV
rc comix 4.0.4-1 GTK Comic Book Viewer
rc gpm 1.20.4-3.2ubuntu2 General Purpose Mouse interface
rc libavcodec52 4:0.5.1-1ubuntu1.1 ffmpeg codec library
rc libavutil49 4:0.5.1-1ubuntu1.1 ffmpeg utility library
rc libgd2-noxpm 2.0.36~rc1~dfsg-3.1ubuntu1 GD Graphics Library version 2 (without XPM support)
rc libucl1 1.03-4build1 Portable compression library - runtime
rc linux-image-2.6.32-28-generic-pae 2.6.32-28.55 Linux kernel image for version 2.6.32 on x86
rc linux-image-2.6.38-rc7 2.6.38-rc7-10.00.Custom Linux kernel binary image for version 2.6.38-rc7
rc linux-image-2.6.38-rc8 2.6.38-rc8-10.00.Custom Linux kernel binary image for version 2.6.38-rc8
rc linux-image-2.6.38.8 2.6.38.8-10.00.Custom Linux kernel binary image for version 2.6.38.8
rc linux-source-2.6.38 2.6.38-10.00.Custom Linux kernel source for version 2.6.38
rc linux-source-2.6.38-rc7 2.6.38-rc7-10.00.Custom Linux kernel source for version 2.6.38-rc7
rc linux-source-2.6.38-rc8 2.6.38-rc8-10.00.Custom Linux kernel source for version 2.6.38-rc8
rc popularity-contest 1.48ubuntu1 Vote for your favourite packages automatically
rc qcomicbook 0.5.0-1 qt viewer for comic book archives (cbr/cbz/cba/cbg/cbb)
rc vsftpd 2.2.2-3ubuntu6.2 lightweight, efficient FTP server written for security
| Status=Not/Inst/Cfg-files/Unpacked/Failed-cfg/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name Version Description

Description

This plugin lists the software installed on the remote host by calling
the appropriate command (rpm -qa on RPM-based Linux distributions,
qpkg, dpkg, etc...)

Solution

Remove any software that is not in compliance with your
organization's acceptable use and security policies.

Risk Factor
None

Plugin publication date: 2006/10/15

Plugin last modification date: 2011/04/22

Port (0/tcp)

Plugin ID: 50686
IP Forwarding Enabled

Synopsis

The remote host has IP forwarding enabled.
List of Hosts

192.168.0.23

Description
The remote host has IP forwarding enabled. An attacker may use this flaw to use the to route packets through this host and potentially bypass some firewalls / routers / NAC filtering.

Unless the remote host is a router, it is recommended that you disable IP forwarding.

Solution
On Linux, you can disable IP forwarding by doing :

echo 0 > /proc/sys/net/ipv4/ip_forward

On Windows, set the key 'IPEnableRouter' to 0 under

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameter

On Mac OS X, you can disable IP forwarding by executing the command :

sysctl -w net.inet.ip.forwarding=0

For other systems, check with your vendor.

Risk Factor
Low/ CVSS Base Score: 3.2
(CVSS2#AV:A/AC:H/Au:N/C:P/I:P/A:N)

CVE
CVE-1999-0511

Plugin publication date: 2010/11/23

Plugin last modification date: 2011/03/21

Port (0/tcp)

Plugin ID: 57616
USN-1335-1 : t1lib vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : libt1-5_5.1.2-3build1
Fixed package : libt1-5_5.1.2-3ubuntu0.10.04.2

Description

Jon Larimer discovered that t1lib did not properly parse AFM fonts. If a user were tricked into using a specially crafted font file, a remote attacker could cause t1lib to crash or possibly execute arbitrary code with user privileges. (CVE-2010-2642, CVE-2011-0433)

Jonathan Brossard discovered that t1lib did not correctly handle certain malformed font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause t1lib to crash. (CVE-2011-1552, CVE-2011-1553, CVE-2011-1554)

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1335-1/

Risk Factor

High/ CVSS Base Score: 7.6
(CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:C)

CVE

CVE-2010-2642
CVE-2011-0433
CVE-2011-1552
CVE-2011-1553
CVE-2011-1554

Other references

USN:1335-1

Patch publication date: 2012/01/19
Plugin publication date: 2012/01/20

Plugin last modification date: 2012/01/20

Port (0/tcp)

Plugin ID: 55689
USN-1174-1 : libsndfile vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : libsndfile1_1.0.21-2
Fixed package : libsndfile1_1.0.21-2ubuntu0.10.04.1

Description
Hossein Lotfi discovered that libsndfile did not properly verify the header length and number of channels for PARIS Audio Format (PAF) audio files. An attacker could exploit this to cause a denial of service via application crash, or possibly execute arbitrary code with the privileges of the user invoking the program.

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1174-1/

Risk Factor
Medium/ CVSS Base Score: 6.8
(CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVE
CVE-2011-2696

Other references
USN:1174-1

Patch publication date: 2011/07/25
Plugin publication date: 2011/07/26

Plugin last modification date: 2011/10/21

Port www (80/tcp)

Plugin ID: 11032
Web Server Directory Enumeration

Synopsis

It is possible to enumerate directories on the web server.
List of Hosts

192.168.0.67
Plugin Output

The following directories were discovered:
/cgi-bin, /icons, /twiki/bin

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

192.168.0.40
Plugin Output

The following directories were discovered:

/cgi-bin, /icons

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

192.168.0.21
Plugin Output

The following directories were discovered:
/cgi-bin, /icons, /php

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

---

Description
This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

Solution
n/a

See also
http://projects.webappsec.org/Predictable-Resource-Location

Risk Factor
None

Other references
OWASP:OWASP-CM-006

Plugin publication date: 2002/06/26

Plugin last modification date: 2011/12/12

Port (0/tcp)

Plugin ID: 57370
USN-1316-1 : t1lib vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

List of Hosts

192.168.0.25

Plugin Output

- Installed package : libt1-5_5.1.2-3build1
Fixed package : libt1-5_5.1.2-3ubuntu0.10.04.1

Description

Jonathan Brossard discovered that t1lib did not correctly handle certain malformed font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause t1lib to crash or possibly execute arbitrary code with user privileges.

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1316-1/

Risk Factor
Medium/ CVSS Base Score: 6.8
(CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVE
CVE-2011-0764

Other references
USN:1316-1

Patch publication date: 2011/12/21
Plugin publication date: 2011/12/22

Plugin last modification date: 2011/12/22

Port (10000/tcp)

Plugin ID: 22964
Service Detection

Synopsis

The remote service could be identified.
List of Hosts

192.168.0.21
Plugin Output
A web server is running on this port.

Description
It was possible to identify the remote service by its banner or by looking

at the error message it sends when it receives an HTTP request.

Solution
n/a

Risk Factor
None

Plugin publication date: 2007/08/19

Plugin last modification date: 2012/01/19

Port www (8834/tcp)

Plugin ID: 22964
Service Detection

Synopsis

The remote service could be identified.
List of Hosts

192.168.0.59
Plugin Output
A web server is running on this port through TLSv1.

192.168.0.59
Plugin Output
A TLSv1 server answered on this port.

192.168.0.54
Plugin Output
A web server is running on this port through TLSv1.

192.168.0.54
Plugin Output
A TLSv1 server answered on this port.

192.168.0.53

Plugin Output
A web server is running on this port through TLSv1.

192.168.0.53
Plugin Output
A TLSv1 server answered on this port.

192.168.0.52
Plugin Output
A web server is running on this port through TLSv1.

192.168.0.52
Plugin Output
A TLSv1 server answered on this port.

192.168.0.41
Plugin Output
A web server is running on this port through TLSv1.

192.168.0.41
Plugin Output
A TLSv1 server answered on this port.

192.168.0.33
Plugin Output
A web server is running on this port through TLSv1.

192.168.0.33
Plugin Output
A TLSv1 server answered on this port.

192.168.0.25
Plugin Output
A web server is running on this port through TLSv1.

192.168.0.25
Plugin Output
A TLSv1 server answered on this port.

192.168.0.24
Plugin Output
A web server is running on this port through TLSv1.

192.168.0.24
Plugin Output
A TLSv1 server answered on this port.

192.168.0.23

Plugin Output
A web server is running on this port through TLSv1.

192.168.0.23
Plugin Output
A TLSv1 server answered on this port.

Description
It was possible to identify the remote service by its banner or by looking
at the error message it sends when it receives an HTTP request.

Solution
n/a

Risk Factor
None

Plugin publication date: 2007/08/19

Plugin last modification date: 2012/01/19

Port (6566/tcp)

Plugin ID: 22964
Service Detection

Synopsis

The remote service could be identified.
List of Hosts

192.168.0.40
Plugin Output
The service closed the connection without sending any data.

It might be protected by some sort of TCP wrapper.

Description
It was possible to identify the remote service by its banner or by looking
at the error message it sends when it receives an HTTP request.

Solution
n/a

Risk Factor
None

Plugin publication date: 2007/08/19

Plugin last modification date: 2012/01/19

Port nessus (1241/tcp)

Plugin ID: 22964
Service Detection

Synopsis

The remote service could be identified.
List of Hosts

192.168.0.59
Plugin Output
A TLSv1 server answered on this port.

192.168.0.54
Plugin Output
A TLSv1 server answered on this port.

192.168.0.53
Plugin Output
A TLSv1 server answered on this port.

192.168.0.52
Plugin Output
A TLSv1 server answered on this port.

192.168.0.41
Plugin Output
A TLSv1 server answered on this port.

192.168.0.33
Plugin Output
A TLSv1 server answered on this port.

192.168.0.25
Plugin Output
A TLSv1 server answered on this port.

192.168.0.24
Plugin Output
A TLSv1 server answered on this port.

192.168.0.23
Plugin Output
A TLSv1 server answered on this port.

Description
It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution
n/a

Risk Factor
None

Plugin publication date: 2007/08/19

Plugin last modification date: 2012/01/19

Port vmware_auth (902/tcp)

Plugin ID: 22964
Service Detection

Synopsis

The remote service could be identified.
List of Hosts

192.168.0.59
Plugin Output
A VMware authentication daemon is running on this port.

192.168.0.54
Plugin Output
A VMware authentication daemon is running on this port.

192.168.0.53
Plugin Output
A VMware authentication daemon is running on this port.

192.168.0.52
Plugin Output
A VMware authentication daemon is running on this port.

192.168.0.41
Plugin Output
A VMware authentication daemon is running on this port.

192.168.0.33
Plugin Output
A VMware authentication daemon is running on this port.

192.168.0.25
Plugin Output
A VMware authentication daemon is running on this port.

192.168.0.24
Plugin Output

A VMware authentication daemon is running on this port.

Description
It was possible to identify the remote service by its banner or by looking
at the error message it sends when it receives an HTTP request.

Solution
n/a

Risk Factor
None

Plugin publication date: 2007/08/19

Plugin last modification date: 2012/01/19

Port (80/tcp)

Plugin ID: 22964
Service Detection

Synopsis

The remote service could be identified.
List of Hosts

192.168.0.67
Plugin Output
A web server is running on this port.

192.168.0.40
Plugin Output
A web server is running on this port.

192.168.0.21
Plugin Output
A web server is running on this port.

Description
It was possible to identify the remote service by its banner or by looking
at the error message it sends when it receives an HTTP request.

Solution
n/a

Risk Factor
None

Plugin publication date: 2007/08/19

Plugin last modification date: 2012/01/19

Port (22/tcp)

Plugin ID: 22964
Service Detection

Synopsis

The remote service could be identified.
List of Hosts

192.168.0.67
Plugin Output
An SSH server is running on this port.

192.168.0.40
Plugin Output

An SSH server is running on this port.

192.168.0.21
Plugin Output
An SSH server is running on this port.

Description
It was possible to identify the remote service by its banner or by looking
at the error message it sends when it receives an HTTP request.

Solution
n/a

Risk Factor
None

Plugin publication date: 2007/08/19

Plugin last modification date: 2012/01/19

Port (0/tcp)

Plugin ID: 55113
USN-1147-1 : gimp vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : gimp_2.6.8-2ubuntu1.2

Fixed package : gimp_2.6.8-2ubuntu1.3

Description
Nils Philippsen discovered that GIMP incorrectly handled malformed PSP image files. If a user were tricked into opening a specially crafted PSP image file, an attacker could cause GIMP to crash, or possibly execute arbitrary code with the user's privileges.

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1147-1/

Risk Factor
High/ CVSS Base Score: 7.5
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVE
CVE-2011-1782

Other references
USN:1147-1

Patch publication date: 2011/06/13
Plugin publication date: 2011/06/14

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 56915
USN-1273-1 : pidgin vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : pidgin_1:2.6.6-1ubuntu4.3
Fixed package : pidgin_1:2.6.6-1ubuntu4.4

Description
Marius Wachtler discovered that Pidgin incorrectly handled malformed YMSG messages in the Yahoo! protocol handler. A remote attacker could send a specially crafted message and cause Pidgin to crash, leading to a denial of service. This issue only affected Ubuntu 10.04 LTS and 10.10. (CVE-2011-1091)

Marius Wachtler discovered that Pidgin incorrectly handled HTTP 100 responses in the MSN protocol handler. A remote attacker could send a specially crafted message and cause Pidgin to crash, leading to a denial of service. (CVE-2011-3184)

Diego Bauche Madero discovered that Pidgin incorrectly handled UTF-8 sequences in the SILC protocol handler. A remote attacker could send a specially crafted message and cause Pidgin to crash, leading to a denial of service. (CVE-2011-3594)

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1273-1/

Risk Factor
Medium/ CVSS Base Score: 4.3
(CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVE
CVE-2011-1091
CVE-2011-3184
CVE-2011-3594

Other references
USN:1273-1

Patch publication date: 2011/11/21
Plugin publication date: 2011/11/21

Plugin last modification date: 2011/11/22

Port (0/tcp)

Plugin ID: 56555
USN-1232-1 : xorg-server vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : xserver-xorg-core_2:1.7.6-2ubuntu7.6
Fixed package : xserver-xorg-core_2:1.7.6-2ubuntu7.8

Description

It was discovered that the X server incorrectly handled certain malformed input. An authorized attacker could exploit this to cause the X server to crash, leading to a denial or service, or possibly execute arbitrary code with root privileges. This issue only affected Ubuntu 10.04 LTS and 10.10. (CVE-2010-4818)

It was discovered that the X server incorrectly handled certain malformed input. An authorized attacker could exploit this to cause the X server to crash, leading to a denial or service, or possibly read arbitrary data from the X server process. This issue only affected Ubuntu 10.04 LTS. (CVE-2010-4819)

Vladz discovered that the X server incorrectly handled lock files. A local attacker could use this flaw to determine if a file existed or not. (CVE-2011-4028)

Vladz discovered that the X server incorrectly handled setting lock file permissions. A local attacker could use this flaw to gain read permissions on arbitrary files and view sensitive information. (CVE-2011-4029)

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1232-1/

Risk Factor

High

CVE

CVE-2010-4818

CVE-2010-4819
CVE-2011-4028
CVE-2011-4029

Other references
USN:1232-1

Patch publication date: 2011/10/18
Plugin publication date: 2011/10/19

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 56468
Time of Last System Startup

Synopsis

The system has been started.
List of Hosts

192.168.0.25
Plugin Output

reboot system boot 2.6.39.4 Sat Jan 28 05:27 - 07:00 (01:33)
reboot system boot 2.6.39.4 Sat Jan 28 03:03 - 03:12 (00:08)
reboot system boot 2.6.39.4 Thu Jan 26 11:28 - 12:49 (01:21)
reboot system boot 2.6.39.4 Thu Jan 26 07:53 - 11:17 (03:24)
reboot system boot 2.6.39.4 Thu Jan 26 04:20 - 07:21 (03:01)
reboot system boot 2.6.39.4 Wed Jan 25 20:49 - 07:21 (10:32)
reboot system boot 2.6.39.4 Wed Jan 25 20:46 - 07:21 (10:35)
reboot system boot 2.6.39.4 Wed Jan 25 19:45 - 20:09 (00:24)
reboot system boot 2.6.39.4 Wed Jan 25 18:31 - 20:09 (01:38)
reboot system boot 2.6.39.4 Tue Jan 24 20:52 - 00:15 (03:22)
reboot system boot 2.6.39.4 Tue Jan 24 09:15 - 12:55 (03:40)
reboot system boot 2.6.39.4 Tue Jan 24 08:57 - 09:05 (00:07)
reboot system boot 2.6.39.4 Tue Jan 24 07:24 - 08:45 (01:21)
reboot system boot 2.6.39.4 Tue Jan 24 05:49 - 06:45 (00:56)
reboot system boot 2.6.38-rc8 Sun Mar 13 08:15 - 08:15 (00:00)

wtmp begins Sun Mar 13 08:15:39 2011

Description
Using the supplied credentials, Nessus was able to determine when the host was last started.

Solution
n/a

Risk Factor
None

Plugin publication date: 2011/10/12

Plugin last modification date: 2011/10/12

Port www (80/tcp)

Plugin ID: 11213
HTTP TRACE / TRACK Methods Allowed

Synopsis

Debugging functions are enabled on the remote web server.
List of Hosts

192.168.0.67
Plugin Output

To disable these methods, add the following lines for each virtual host in your configuration file :

RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)

RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Nessus sent the following TRACE request :

```
------------------------------ snip ------------------------------
TRACE /Nessus685465018.html HTTP/1.1
Connection: Close
Host: 192.168.0.67
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------
```

and received the following response from the remote server :

```
------------------------------ snip ------------------------------
HTTP/1.1 200 OK
Date: Fri, 27 Jan 2012 23:08:19 GMT
Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http


TRACE /Nessus685465018.html HTTP/1.1
Connection: Keep-Alive
Host: 192.168.0.67
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------
```

192.168.0.21
Plugin Output

To disable these methods, add the following lines for each virtual
host in your configuration file :

RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Nessus sent the following TRACE request :

------------------------------ snip ------------------------------
TRACE /Nessus1997936744.html HTTP/1.1
Connection: Close
Host: 192.168.0.21
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------

and received the following response from the remote server :

------------------------------ snip ------------------------------
HTTP/1.1 200 OK
Date: Fri, 27 Jan 2012 22:51:53 GMT
Server: Apache/2.2.4 (Ubuntu) PHP/5.2.3-1ubuntu6
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: message/http

TRACE /Nessus1997936744.html HTTP/1.1
Connection: Keep-Alive
Host: 192.168.0.21
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8

------------------------------ snip ------------------------------

---

Description

The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

Solution

Disable these methods. Refer to the plugin output for more information.

See also

http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf
http://www.apacheweek.com/issues/03-01-24
http://www.kb.cert.org/vuls/id/288308
http://www.kb.cert.org/vuls/id/867593
http://download.oracle.com/sunalerts/1000718.1.html

Risk Factor

Medium/ CVSS Base Score: 4.3
(CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)
CVSS Temporal Score: 3.9(CVSS2#E:F/RL:W/RC:C)

CVE

CVE-2003-1567
CVE-2004-2320
CVE-2010-0386

Bugtraq ID

9506
9561
11604
33374
37995

Other references
OSVDB:877
OSVDB:3726
OSVDB:5648
OSVDB:50485
CWE:16

Vulnerability publication date: 2003/01/20
Plugin publication date: 2003/01/23
Plugin last modification date: 2011/09/19

Ease of exploitability: Exploits are available

Port (0/tcp)

Plugin ID: 56554
USN-1231-1 : php5 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : libapache2-mod-php5_5.3.2-1ubuntu4.9
Fixed package : libapache2-mod-php5_5.3.2-1ubuntu4.10

- Installed package : php5-cgi_5.3.2-1ubuntu4.9
Fixed package : php5-cgi_5.3.2-1ubuntu4.10

- Installed package : php5-cli_5.3.2-1ubuntu4.9
Fixed package : php5-cli_5.3.2-1ubuntu4.10

- Installed package : php5-common_5.3.2-1ubuntu4.9
Fixed package : php5-common_5.3.2-1ubuntu4.10

Description

Mateusz Kocielski, Marek Kroemeke and Filip Palian discovered that a stack-based buffer overflow existed in the socket_connect function's handling of long pathnames for AF_UNIX sockets. A remote attacker might be able to exploit this to execute arbitrary code; however, the default compiler options for affected releases should reduce the vulnerability to a denial of service. This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10 and Ubuntu 11.04. (CVE-2011-1938)

Krzysztof Kotowicz discovered that the PHP post handler function does not properly restrict filenames in multipart/form-data POST requests. This may allow remote attackers to conduct absolute path traversal attacks and possibly create or overwrite arbitrary files. This issue affected Ubuntu 8.04 LTS, Ubuntu 10.04 LTS, Ubuntu 10.10 and Ubuntu 11.04. (CVE-2011-2202)

It was discovered that the crypt function for blowfish does not properly handle 8-bit characters. This could make it easier for an attacker to discover a cleartext password containing an 8-bit character that has a matching blowfish crypt value. This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10 and Ubuntu 11.04. (CVE-2011-2483)

It was discovered that PHP did not properly check the return values of the malloc(3), calloc(3) and realloc(3) library functions in multiple locations. This could allow an attacker to cause a denial of service via a NULL pointer dereference or possibly execute arbitrary code. This issue affected Ubuntu 8.04 LTS, Ubuntu 10.04 LTS, Ubuntu 10.10 and Ubuntu 11.04. (CVE-2011-3182)

Maksymilian Arciemowicz discovered that PHP did not properly implement the error_log function. This could allow an attacker to cause a denial of service via an application crash. This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10, Ubuntu 11.04 and Ubuntu 11.10. (CVE-2011-3267)

Maksymilian Arciemowicz discovered that the ZipArchive functions addGlob() and addPattern() did not properly check their flag arguments. This could allow a malicious script author to cause a denial of service via application crash. This issue affected Ubuntu 10.04 LTS, Ubuntu 10.10, Ubuntu 11.04 and Ubuntu 11.10. (CVE-2011-1657)

It was discovered that the Xend opcode parser in PHP could be

interrupted while handling the shift-left, shift-right, and bitwise-xor opcodes. This could allow a malicious script author to expose memory contents. This issue affected Ubuntu 10.04 LTS. (CVE-2010-1914)

It was discovered that the strrchr function in PHP could be interrupted by a malicious script, allowing the exposure of memory contents. This issue affected Ubuntu 8.04 LTS. (CVE-2010-2484)

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1231-1/

Risk Factor

High/ CVSS Base Score: 7.5
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVE

CVE-2010-1914
CVE-2010-2484
CVE-2011-1657
CVE-2011-1938
CVE-2011-2202
CVE-2011-2483
CVE-2011-3182
CVE-2011-3267

Other references

USN:1231-1

Patch publication date: 2011/10/18
Plugin publication date: 2011/10/19

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 55097
USN-1136-1 : rdesktop vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : rdesktop_1.6.0-2ubuntu3
Fixed package : rdesktop_1.6.0-2ubuntu3.1

Description
It was discovered that rdesktop incorrectly handled specially crafted paths when using disk redirection. If a user were tricked into connecting to a malicious server, an attacker could access arbitrary files on the user's filesystem.

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1136-1/

Risk Factor

Medium/ CVSS Base Score: 4.3
(CVSS2#AV:A/AC:H/Au:N/C:P/I:P/A:P)

CVE
CVE-2011-1595

Other references
USN:1136-1

Patch publication date: 2011/05/25
Plugin publication date: 2011/06/13

Plugin last modification date: 2011/10/21

Port www (8834/tcp)

Plugin ID: 57582
SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.
List of Hosts

192.168.0.59
Plugin Output

The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority

192.168.0.54
Plugin Output

The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not

found in the list of known certificate authorities :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority

192.168.0.53
Plugin Output

The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority

192.168.0.52
Plugin Output

The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority

192.168.0.41
Plugin Output

The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority

192.168.0.33
Plugin Output

The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority

192.168.0.25
Plugin Output

The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority

192.168.0.24
Plugin Output

The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority

192.168.0.23
Plugin Output

The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority

---

Description
The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man in the middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution
Purchase or generate a proper certificate for this service.

Risk Factor
Medium/ CVSS Base Score: 6.4
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin publication date: 2012/01/17

Plugin last modification date: 2012/01/17

Port nessus (1241/tcp)

Plugin ID: 57582
SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.
List of Hosts

192.168.0.54
Plugin Output

The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New
York/C=US/ST=NY/CN=Nessus Certification Authority

192.168.0.53
Plugin Output

The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New
York/C=US/ST=NY/CN=Nessus Certification Authority

192.168.0.33
Plugin Output

The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority

192.168.0.25
Plugin Output

The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority

192.168.0.24
Plugin Output

The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority

192.168.0.23
Plugin Output

The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority

---

Description
The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man in the middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution
Purchase or generate a proper certificate for this service.

Risk Factor
Medium/ CVSS Base Score: 6.4
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin publication date: 2012/01/17

Plugin last modification date: 2012/01/17

Port (0/tcp)

Plugin ID: 56970
USN-1283-1 : apt vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : apt_0.7.25.3ubuntu9.4
Fixed package : apt_0.7.25.3ubuntu9.9

Description
It was discovered that APT incorrectly handled the Verify-Host

configuration option. If a remote attacker were able to perform a man-in-the-middle attack, this flaw could potentially be used to steal repository credentials. This issue only affected Ubuntu 10.04 LTS and 10.10. (CVE-2011-3634)

USN-1215-1 fixed a vulnerability in APT by disabling the apt-key net-update option. This update re-enables the option with corrected verification. Original advisory details: It was discovered that the apt-key utility incorrectly verified GPG keys when downloaded via the net-update option. If a remote attacker were able to perform a man-in-the-middle attack, this flaw could potentially be used to install altered packages.

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1283-1/

Risk Factor

High

CVE

CVE-2011-3634

Other references

USN:1283-1

Patch publication date: 2011/11/28
Plugin publication date: 2011/11/29

Plugin last modification date: 2011/11/29

Port nessus (1241/tcp)

Plugin ID: 10147
Nessus Server Detection

Synopsis

A Nessus daemon is listening on the remote port.

List of Hosts

192.168.0.59

192.168.0.54

192.168.0.53

192.168.0.52

192.168.0.41

192.168.0.33

192.168.0.25

192.168.0.24

192.168.0.23

Description

A Nessus daemon is listening on the remote port. It is not recommended to let anyone connect to this port.

Also, make sure that the remote Nessus installation has been authorized.

Solution

Filter incoming traffic to this port.

Risk Factor
None

Plugin publication date: 1999/10/12

Plugin last modification date: 2011/03/11

Port (0/tcp)

Plugin ID: 18261
Apache Banner Linux Distribution Disclosure

Synopsis

The name of the Linux distribution running on the remote host was found in the banner of the web server.
List of Hosts

192.168.0.67
Plugin Output

The linux distribution detected was :
- Ubuntu 8.04 (gutsy)

192.168.0.40
Plugin Output

The linux distribution detected was :
- Ubuntu 10.10 (maverick)

Description
This script extracts the banner of the Apache web server and attempts to determine which Linux distribution the remote host is running.

Solution
If you do not wish to display this information, edit httpd.conf and set the directive 'ServerTokens Prod' and restart Apache.

Risk Factor
None

Plugin publication date: 2005/05/15

Plugin last modification date: 2012/01/24

Port cifs (445/tcp)

Plugin ID: 17651
Microsoft Windows SMB : Obtains the Password Policy

Synopsis

It is possible to retrieve the remote host's password policy using the supplied credentials.
List of Hosts

192.168.0.67
Plugin Output
The following password policy is defined on the remote host:

Minimum password len: 5
Password history len: 0
Maximum password age (d): No limit
Password must meet complexity requirements: Disabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 1800
Number of invalid logon before locked out (s): 0

192.168.0.59
Plugin Output
The following password policy is defined on the remote host:

Minimum password len: 5
Password history len: 0
Maximum password age (d): No limit
Password must meet complexity requirements: Disabled
Minimum password age (d): 0

Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 1800
Number of invalid logon before locked out (s): 0

192.168.0.54
Plugin Output
The following password policy is defined on the remote host:

Minimum password len: 5
Password history len: 0
Maximum password age (d): No limit
Password must meet complexity requirements: Disabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 1800
Number of invalid logon before locked out (s): 0

192.168.0.53
Plugin Output
The following password policy is defined on the remote host:

Minimum password len: 5
Password history len: 0
Maximum password age (d): No limit
Password must meet complexity requirements: Disabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 1800
Number of invalid logon before locked out (s): 0

192.168.0.52
Plugin Output
The following password policy is defined on the remote host:

Minimum password len: 5
Password history len: 0
Maximum password age (d): No limit
Password must meet complexity requirements: Disabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 1800
Number of invalid logon before locked out (s): 0

192.168.0.41

Plugin Output
The following password policy is defined on the remote host:

Minimum password len: 5
Password history len: 0
Maximum password age (d): No limit
Password must meet complexity requirements: Disabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 1800
Number of invalid logon before locked out (s): 0

192.168.0.33
Plugin Output
The following password policy is defined on the remote host:

Minimum password len: 5
Password history len: 0
Maximum password age (d): No limit
Password must meet complexity requirements: Disabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 1800
Number of invalid logon before locked out (s): 0

192.168.0.25
Plugin Output
The following password policy is defined on the remote host:

Minimum password len: 5
Password history len: 0
Maximum password age (d): No limit
Password must meet complexity requirements: Disabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 1800
Number of invalid logon before locked out (s): 0

192.168.0.24
Plugin Output
The following password policy is defined on the remote host:

Minimum password len: 5
Password history len: 0
Maximum password age (d): No limit

Password must meet complexity requirements: Disabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 1800
Number of invalid logon before locked out (s): 0

192.168.0.21
Plugin Output
The following password policy is defined on the remote host:

Minimum password len: 5
Password history len: 0
Maximum password age (d): No limit
Password must meet complexity requirements: Disabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 1800
Number of invalid logon before locked out (s): 0

Description
Using the supplied credentials it was possible to extract the password policy for the remote Windows host. The password policy must conform to the Informational System Policy.

Solution
n/a

Risk Factor
None

Plugin publication date: 2005/03/30

Plugin last modification date: 2011/03/04

Port (0/tcp)

Plugin ID: 55103
USN-1140-2 : pam regression

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : libpam-modules_1.1.1-2ubuntu5.1
Fixed package : libpam-modules_1.1.1-2ubuntu5.3

- Installed package : libpam0g_1.1.1-2ubuntu5.1
Fixed package : libpam0g_1.1.1-2ubuntu5.3

Description
USN-1140-1 fixed vulnerabilities in PAM. A regression was found that caused cron to stop working with a 'Module is unknown' error. As a result, systems configured with automatic updates will not receive updates until cron is restarted, these updates are installed or the system is rebooted. This update fixes the problem.

We apologize for the inconvenience.

Original advisory details:

Marcus Granado discovered that PAM incorrectly handled configuration files with non-ASCII usernames. A remote attacker could use this flaw to cause a denial of service, or possibly obtain login access with a different users username. This issue only affected Ubuntu 8.04 LTS. (CVE-2009-0887)

It was discovered that the PAM pam_xauth, pam_env and pam_mail modules incorrectly handled dropping privileges when performing operations. A local attacker could use this flaw to read certain arbitrary files, and access other sensitive information. (CVE-2010-3316, CVE-2010-3430, CVE-2010-3431, CVE-2010-3435)

It was discovered that the PAM pam_namespace module incorrectly cleaned the environment during execution of the namespace.init script. A local attacker could use this flaw to possibly gain privileges. (CVE-2010-3853)

It was discovered that the PAM pam_xauth module incorrectly handled certain failures. A local attacker could use this flaw to delete certain unintended files. (CVE-2010-4706)

It was discovered that the PAM pam_xauth module incorrectly verified certain file properties. A local attacker could use this flaw to cause a denial of service. (CVE-2010-4707)

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1140-2/

Risk Factor

Medium/ CVSS Base Score: 6.9
(CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

CVE

CVE-2009-0887
CVE-2010-3316
CVE-2010-3430
CVE-2010-3431
CVE-2010-3435
CVE-2010-3853
CVE-2010-4706
CVE-2010-4707

Other references

USN:1140-2
CWE:189

Patch publication date: 2011/05/31
Plugin publication date: 2011/06/13

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 55605
USN-1150-1 : thunderbird vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : thunderbird_3.1.10+build1+nobinonly-0ubuntu0.10.04.1
Fixed package : thunderbird_3.1.11+build2+nobinonly-0ubuntu0.10.04.1

Description
Multiple memory vulnerabilities were discovered in the browser
rendering engine. An attacker could use these to possibly execute
arbitrary code with the privileges of the user invoking Thunderbird.
(CVE-2011-2364, CVE-2011-2365, CVE-2011-2374, CVE-2011-2376)

Martin Barbella discovered that under certain conditions, viewing a
XUL document while JavaScript was disabled caused deleted memory to
be accessed. An attacker could potentially use this to crash
Thunderbird or execute arbitrary code with the privileges of the user
invoking Thunderbird. (CVE-2011-2373)

Jordi Chancel discovered a vulnerability on multipart/x-mixed-replace
images due to memory corruption. An attacker could potentially use
this to crash Thunderbird or execute arbitrary code with the

privileges of the user invoking Thunderbird. (CVE-2011-2377)

Chris Rohlf and Yan Ivnitskiy discovered an integer overflow vulnerability in JavaScript Arrays. An attacker could potentially use this to execute arbitrary code with the privileges of the user invoking Thunderbird. (CVE-2011-2371)

Multiple use-after-free vulnerabilities were discovered. An attacker could potentially use these to execute arbitrary code with the privileges of the user invoking Thunderbird. (CVE-2011-0083, CVE-2011-0085, CVE-2011-2363)

David Chan discovered that cookies did not honor same-origin conventions. This could potentially lead to cookie data being leaked to a third party. (CVE-2011-2362)

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1150-1/

Risk Factor

Critical/ CVSS Base Score: 10.0
(CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVE

CVE-2011-0083
CVE-2011-0085
CVE-2011-2362
CVE-2011-2363
CVE-2011-2364
CVE-2011-2365
CVE-2011-2371
CVE-2011-2373
CVE-2011-2374
CVE-2011-2376
CVE-2011-2377

Other references
USN:1150-1

Patch publication date: 2011/07/15
Plugin publication date: 2011/07/18
Plugin last modification date: 2011/10/21
Ease of exploitability: Exploits are available

Exploitable with: Metasploit (windows/browser/mozilla_reduceright.rb)

Port cifs (445/tcp)

Plugin ID: 25216
Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow

Synopsis

It is possible to execute code on the remote host through Samba.
List of Hosts

192.168.0.67

Description
The version of the Samba server installed on the remote host is affected by multiple heap overflow vulnerabilities, which can be exploited remotely to execute code with the privileges of the Samba daemon.

Solution
Upgrade to Samba version 3.0.25 or later.

See also
http://www.samba.org/samba/security/CVE-2007-2446.html

Risk Factor
Critical/ CVSS Base Score: 10.0
(CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVE
CVE-2007-2446

Bugtraq ID
23973
24195
24196
24197
24198

Other references
OSVDB:34699
OSVDB:34731
OSVDB:34732
OSVDB:34733

Vulnerability publication date: 2007/05/14
Patch publication date: 2007/07/11
Plugin publication date: 2007/05/15
Plugin last modification date: 2011/04/13
Ease of exploitability: Exploits are available

Exploitable with: Canvas (CANVAS), Metasploit (Samba lsa_io_trans_names Heap Overflow)

Port (0/tcp)

Plugin ID: 56861
USN-1264-1 : bind9 vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

List of Hosts

192.168.0.25

Plugin Output

- Installed package : libdns64_1:9.7.0.dfsg.P1-1ubuntu0.1
Fixed package : libdns64_1:9.7.0.dfsg.P1-1ubuntu0.4

Description

It was discovered that Bind incorrectly handled certain specially crafted packets. A remote attacker could use this flaw to cause Bind to crash, resulting in a denial of service.

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1264-1/

Risk Factor

Medium/ CVSS Base Score: 5.0
(CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVE

CVE-2011-4313

Other references

IAVA:2011-A-0158
USN:1264-1

Patch publication date: 2011/11/16
Plugin publication date: 2011/11/17

Plugin last modification date: 2011/12/12

Port www (10000/tcp)

Plugin ID: 22300
Webmin / Usermin Null Byte Filtering Vulnerabilities

Synopsis

The remote web server is affected by multiple issues.
List of Hosts

192.168.0.21

Description
The remote host is running Webmin or Usermin, web-based interfaces for Unix / Linux system administrators and end-users.

Webmin and Usermin both come with the Perl script 'miniserv.pl' to provide basic web services, and the version of 'miniserv.pl' installed on the remote host fails to properly filter null characters from URLs. An attacker may be able to exploit this to reveal the source code of CGI scripts, obtain directory listings, or launch cross-site scripting attacks against the affected application.

Solution
Upgrade to Webmin version 1.296 / Usermin 1.226 or later.

See also
http://www.lac.co.jp/business/sns/intelligence/SNSadvisory_e/89_e.html

http://www.webmin.com/security.html

Risk Factor
Medium/ CVSS Base Score: 6.8
(CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)
CVSS Temporal Score: 6.5(CVSS2#E:F/RL:U/RC:C)

CVE
CVE-2006-4542

Bugtraq ID
19820

Other references
OSVDB:28337
OSVDB:28338

Vulnerability publication date: 2006/09/01
Plugin publication date: 2006/09/02
Plugin last modification date: 2011/03/14

Ease of exploitability: Exploits are available

Port (0/tcp)

Plugin ID: 57393
USN-1254-1 : thunderbird vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25

Plugin Output

- Installed package : thunderbird_3.1.10+build1+nobinonly-0ubuntu0.10.04.1
Fixed package : thunderbird_3.1.16+build2+nobinonly-0ubuntu0.10.04.1

Description

It was discovered that CVE-2011-3004, which addressed possible privilege escalation in addons, also affected Thunderbird 3.1. An attacker could potentially exploit a user who had installed an add-on that used loadSubscript in vulnerable ways. (CVE-2011-3647)

Yosuke Hasegawa discovered that the Mozilla browser engine mishandled invalid sequences in the Shift-JIS encoding. It may be possible to trigger this crash without the use of debugging APIs, which might allow malicious websites to exploit this vulnerability. An attacker could possibly use this flaw this to steal data or inject malicious scripts into web content. (CVE-2011-3648)

Marc Schoenefeld discovered that using Firebug to profile a JavaScript file with many functions would cause Firefox to crash. An attacker might be able to exploit this without using the debugging APIs which would potentially allow an attacker to remotely crash Thunderbird. (CVE-2011-3650)

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1254-1/

Risk Factor

High/ CVSS Base Score: 9.3
(CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVE
CVE-2011-3004
CVE-2011-3647
CVE-2011-3648
CVE-2011-3650

Other references
IAVA:2011-A-0133
IAVA:2011-A-0154
USN:1254-1

Patch publication date: 2011/12/22
Plugin publication date: 2011/12/23

Plugin last modification date: 2011/12/27

Port (0/tcp)

Plugin ID: 55100
USN-1138-2 : network-manager, modemmanger update

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : libnm-glib2_0.8-0ubuntu3
Fixed package : libnm-glib2_0.8-0ubuntu3.2

Description

USN-1138-1 fixed a vulnerability in DBus-GLib. NetworkManager and ModemManager required rebuilding against the updated DBus-GLib to incorporate the changes.

Original advisory details:

It was discovered that DBus-GLib did not properly verify the access flag of exported GObject properties under certain circumstances. A local attacker could exploit this to bypass intended access restrictions or possibly cause a denial of service.

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1138-2/

Risk Factor
High

Other references
USN:1138-2

Patch publication date: 2011/05/27
Plugin publication date: 2011/06/13

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 56331
USN-1213-1 : thunderbird vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : thunderbird_3.1.10+build1+nobinonly-0ubuntu0.10.04.1
Fixed package : thunderbird_3.1.15+build1+nobinonly-0ubuntu0.10.04.1

Description
Benjamin Smedberg, Bob Clary, Jesse Ruderman, and Josh Aas discovered multiple memory vulnerabilities in the Gecko rendering engine. An attacker could use these to possibly execute arbitrary code with the privileges of the user invoking Thunderbird. (CVE-2011-2995, CVE-2011-2996)

Boris Zbarsky discovered that a frame named 'location' could shadow the window.location object unless a script in a page grabbed a reference to the true object before the frame was created. This is in violation of the Same Origin Policy. A malicious E-Mail could possibly use this to access the local file system. (CVE-2011-2999)

Mark Kaplan discovered an integer underflow in the SpiderMonkey JavaScript engine. An attacker could potentially use this to crash Thunderbird.

Ian Graham discovered that when multiple Location headers were present, Thunderbird would use the second one resulting in a possible CRLF injection attack. CRLF injection issues can result in a wide variety of attacks, such as XSS (Cross-Site Scripting) vulnerabilities, browser cache poisoning, and cookie theft. (CVE-2011-3000)

Mariusz Mlynski discovered that if the user could be convinced to hold down the enter key, a malicious website or E-Mail could potential pop up a download dialog and the default open action would be selected. This would result in potentially malicious content being run with privileges of the user invoking Thunderbird. (CVE-2011-2372)

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1213-1/

Risk Factor
Critical/ CVSS Base Score: 10.0
(CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVE
CVE-2011-2372
CVE-2011-2995
CVE-2011-2996
CVE-2011-2999
CVE-2011-3000

Other references
IAVA:2011-A-0133
USN:1213-1

Patch publication date: 2011/09/28
Plugin publication date: 2011/09/29

Plugin last modification date: 2011/12/12

Port (0/tcp)

Plugin ID: 55095
USN-1134-1 : apache2, apr vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

List of Hosts

192.168.0.25
Plugin Output

- Installed package : libapr1_1.3.8-1build1
Fixed package : libapr1_1.3.8-1ubuntu0.3

Description
Maksymilian Arciemowicz reported that a flaw in the fnmatch() implementation in the Apache Portable Runtime (APR) library could allow an attacker to cause a denial of service. This can be demonstrated in a remote denial of service attack against mod_autoindex in the Apache web server. (CVE-2011-0419)

Is was discovered that the fix for CVE-2011-0419 introduced a different flaw in the fnmatch() implementation that could also result in a denial of service. (CVE-2011-1928)

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1134-1/

Risk Factor
Medium/ CVSS Base Score: 4.3
(CVSS2#AV:N/AC:M/Au:N/C:N/I:N/A:P)

CVE
CVE-2011-0419
CVE-2011-1928

Other references
USN:1134-1

Patch publication date: 2011/05/24
Plugin publication date: 2011/06/13

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 55102
USN-1140-1 : pam vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : libpam-modules_1.1.1-2ubuntu5.1
Fixed package : libpam-modules_1.1.1-2ubuntu5.2

Description
Marcus Granado discovered that PAM incorrectly handled configuration files with non-ASCII usernames. A remote attacker could use this flaw to cause a denial of service, or possibly obtain login access with a different users username. This issue only affected Ubuntu 8.04 LTS. (CVE-2009-0887)

It was discovered that the PAM pam_xauth, pam_env and pam_mail modules incorrectly handled dropping privileges when performing operations. A local attacker could use this flaw to read certain arbitrary files, and access other sensitive information. (CVE-2010-3316, CVE-2010-3430, CVE-2010-3431, CVE-2010-3435)

It was discovered that the PAM pam_namespace module incorrectly cleaned the environment during execution of the namespace.init script. A local attacker could use this flaw to possibly gain privileges. (CVE-2010-3853)

It was discovered that the PAM pam_xauth module incorrectly handled certain failures. A local attacker could use this flaw to delete certain unintended files. (CVE-2010-4706)

It was discovered that the PAM pam_xauth module incorrectly verified certain file properties. A local attacker could use this flaw to cause a denial of service. (CVE-2010-4707)

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1140-1/

Risk Factor

Medium/ CVSS Base Score: 6.9
(CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

CVE

CVE-2009-0887
CVE-2010-3316
CVE-2010-3430
CVE-2010-3431
CVE-2010-3435
CVE-2010-3853
CVE-2010-4706
CVE-2010-4707

Other references

USN:1140-1
CWE:189

Patch publication date: 2011/05/30
Plugin publication date: 2011/06/13

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 56870
USN-1267-1 : freetype vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : libfreetype6_2.3.11-1ubuntu2.4
Fixed package : libfreetype6_2.3.11-1ubuntu2.5

Description
It was discovered that FreeType did not correctly handle certain malformed Type 1 font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash or possibly execute arbitrary code with user privileges. (CVE-2011-3256)

It was discovered that FreeType did not correctly handle certain malformed CID-keyed PostScript font files. If a user were tricked into using a specially crafted font file, a remote attacker could cause FreeType to crash or possibly execute arbitrary code with user privileges. (CVE-2011-3439)

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1267-1/

Risk Factor
High/ CVSS Base Score: 9.3
(CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVE
CVE-2011-3256
CVE-2011-3439

Other references
USN:1267-1

Patch publication date: 2011/11/18
Plugin publication date: 2011/11/18

Plugin last modification date: 2011/11/18

Port (0/tcp)

Plugin ID: 56775
USN-1251-1 : firefox, xulrunner-1.9.2 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : xulrunner-1.9.2_1.9.2.17+build3+nobinonly-0ubuntu0.10.04.1
Fixed package : xulrunner-1.9.2_1.9.2.24+build2+nobinonly-0ubuntu0.10.04.1

Description

It was discovered that CVE-2011-3004, which addressed possible privilege escalation in addons, also affected Firefox 3.6. An attacker could potentially exploit Firefox when an add-on was installed that used loadSubscript in vulnerable ways. (CVE-2011-3647)

Yosuke Hasegawa discovered that the Mozilla browser engine mishandled invalid sequences in the Shift-JIS encoding. A malicious website could possibly use this flaw this to steal data or inject malicious scripts into web content. (CVE-2011-3648)

Marc Schoenefeld discovered that using Firebug to profile a JavaScript file with many functions would cause Firefox to crash. An attacker might be able to exploit this without using the debugging APIs which would potentially allow an attacker to remotely crash the browser. (CVE-2011-3650)

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1251-1/

Risk Factor

High/ CVSS Base Score: 9.3
(CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVE

CVE-2011-3004

CVE-2011-3647
CVE-2011-3648
CVE-2011-3650

Other references
IAVA:2011-A-0133
IAVA:2011-A-0154
USN:1251-1

Patch publication date: 2011/11/10
Plugin publication date: 2011/11/11

Plugin last modification date: 2011/12/12

Port (0/tcp)

Plugin ID: 57663
USN-1339-1 : qemu-kvm vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : qemu-kvm_0.12.3+noroms-0ubuntu9.6
Fixed package : qemu-kvm_0.12.3+noroms-0ubuntu9.17

Description
Nicolae Mogoreanu discovered that QEMU did not properly verify legacy mode packets in the e1000 network driver. A remote attacker could exploit this to cause a denial of service or possibly execute code with the privileges of the user invoking the program.

When using QEMU with libvirt or virtualization management software

based on libvirt such as Eucalyptus and OpenStack, QEMU guests are individually isolated by an AppArmor profile by default in Ubuntu.

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1339-1/

Risk Factor
High

CVE
CVE-2012-0029

Other references
USN:1339-1

Patch publication date: 2012/01/23
Plugin publication date: 2012/01/24

Plugin last modification date: 2012/01/24

Port (0/tcp)

Plugin ID: 52740
USN-1090-1 : linux vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

List of Hosts

192.168.0.25
Plugin Output

- Installed package : linux-libc-dev_2.6.32-29.58
Fixed package : linux-libc-dev_2.6.32-30.59

Description
Dan Rosenberg discovered that multiple terminal ioctls did not correctly initialize structure memory. A local attacker could exploit this to read portions of kernel stack memory, leading to a loss of privacy. (CVE-2010-4076, CVE-2010-4077)

Dan Rosenberg discovered that the socket filters did not correctly initialize structure memory. A local attacker could create malicious filters to read portions of kernel stack memory, leading to a loss of privacy. (Ubuntu 10.10 was already fixed in a prior update.) (CVE-2010-4158)

Dan Rosenberg discovered that the SCSI subsystem did not correctly validate iov segments. A local attacker with access to a SCSI device could send specially crafted requests to crash the system, leading to a denial of service. (CVE-2010-4163)

Dan Rosenberg discovered that the RDS protocol did not correctly check ioctl arguments. A local attacker could exploit this to crash the system, leading to a denial of service. (CVE-2010-4175)

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1090-1/

Risk Factor

Medium/ CVSS Base Score: 4.9
(CVSS2#AV:L/AC:L/Au:N/C:N/I:N/A:C)

CVE
CVE-2010-4076
CVE-2010-4077
CVE-2010-4158
CVE-2010-4163
CVE-2010-4175

Other references
USN:1090-1

Patch publication date: 2011/03/18
Plugin publication date: 2011/03/21

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 56767
USN-1255-1 : libmodplug vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : libmodplug0c2_1:0.8.7-1build1
Fixed package : libmodplug0c2_1:0.8.7-1ubuntu0.3

Description

Hossein Lotfi discovered that libmodplug did not correctly handle certain malformed media files. If a user or automated system were tricked into opening a crafted media file, an attacker could cause a denial of service or possibly execute arbitrary code with privileges of the user invoking the program. (CVE-2011-2911, CVE-2011-2912, CVE-2011-2913)

It was discovered that libmodplug did not correctly handle certain malformed media files. If a user or automated system were tricked into opening a crafted media file, an attacker could cause a denial of service or possibly execute arbitrary code with privileges of the user invoking the program. (CVE-2011-2914, CVE-2011-2915)

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1255-1/

Risk Factor

High

CVE

CVE-2011-2911
CVE-2011-2912
CVE-2011-2913
CVE-2011-2914
CVE-2011-2915

Other references

USN:1255-1

Patch publication date: 2011/11/09
Plugin publication date: 2011/11/10

Plugin last modification date: 2011/11/10

Port www (80/tcp)

Plugin ID: 40665
Protected Web Page Detection

Synopsis

Some web pages require authentication.

List of Hosts

192.168.0.21

Plugin Output

The following pages are protected by the Basic authentication scheme :

/php/phpMyAdmin/
/php/phpMyAdmin/?D=A

Description

The remote web server requires HTTP authentication for the following pages. Several authentication schemes are available :

- Basic is the simplest but the credential are sent in clear text.

- NTLM provides an SSO in MS environment, but it cannot be used on both the proxy and the web server. It is also weaker than Digest.

- Digest is a cryptographically strong scheme. Credentials are never sent in clear text. They may still be cracked by a dictionary attack though.

Solution

n/a

Risk Factor
None

Plugin publication date: 2009/08/21

Plugin last modification date: 2011/03/15

Port (0/tcp)

Plugin ID: 56563
USN-1232-2 : xorg-server regression

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : xserver-xorg-core_2:1.7.6-2ubuntu7.6
Fixed package : xserver-xorg-core_2:1.7.6-2ubuntu7.9

Description
USN-1232-1 fixed vulnerabilities in the X.Org X server. A regression was found on Ubuntu 10.04 LTS that affected GLX support.

This update temporarily disables the fix for CVE-2010-4818 that introduced the regression.

We apologize for the inconvenience.

Original advisory details:

It was discovered that the X server incorrectly handled certain

malformed input. An authorized attacker could exploit this to cause the X server to crash, leading to a denial or service, or possibly execute arbitrary code with root privileges. This issue only affected Ubuntu 10.04 LTS and 10.10. (CVE-2010-4818)

It was discovered that the X server incorrectly handled certain malformed input. An authorized attacker could exploit this to cause the X server to crash, leading to a denial or service, or possibly read arbitrary data from the X server process. This issue only affected Ubuntu 10.04 LTS. (CVE-2010-4819)

Vladz discovered that the X server incorrectly handled lock files. A local attacker could use this flaw to determine if a file existed or not. (CVE-2011-4028)

Vladz discovered that the X server incorrectly handled setting lock file permissions. A local attacker could use this flaw to gain read permissions on arbitrary files and view sensitive information. (CVE-2011-4029)

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1232-2/

Risk Factor

High

CVE

CVE-2010-4818
CVE-2010-4819
CVE-2011-4028
CVE-2011-4029

Other references
USN:1232-2

Patch publication date: 2011/10/19
Plugin publication date: 2011/10/20

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 56036
USN-1197-1 : firefox, xulrunner-1.9.2 vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : xulrunner-1.9.2_1.9.2.17+build3+nobinonly-0ubuntu0.10.04.1
Fixed package : xulrunner-1.9.2_1.9.2.21+build1+nobinonly-0ubuntu0.10.04.1

Description
It was discovered that Dutch Certificate Authority DigiNotar, had mis-issued multiple fraudulent certificates. These certificates could allow an attacker to perform a 'man in the middle' (MITM) attack which would make the user believe their connection is secure, but is actually being monitored.

For the protection of its users, Mozilla has removed the DigiNotar certificate. Sites using certificates issued by DigiNotar will need to seek another certificate vendor.

We are currently aware of a regression that blocks one of two Staat der Nederlanden root certificates which are believed to still be secure. This regression is being tracked at https://launchpad.net/bugs/838322.

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1197-1/

Risk Factor
High

Other references
USN:1197-1

Patch publication date: 2011/09/01
Plugin publication date: 2011/09/01

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 55172
USN-1154-1 : openjdk-6, openjdk-6b18 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : openjdk-6-jre_6b20-1.9.7-0ubuntu1~10.04.1
Fixed package : openjdk-6-jre_6b20-1.9.8-0ubuntu1~10.04.1

- Installed package : openjdk-6-jre-headless_6b20-1.9.7-0ubuntu1~10.04.1
Fixed package : openjdk-6-jre-headless_6b20-1.9.8-0ubuntu1~10.04.1

- Installed package : openjdk-6-jre-lib_6b20-1.9.7-0ubuntu1~10.04.1
Fixed package : openjdk-6-jre-lib_6b20-1.9.8-0ubuntu1~10.04.1

Description

It was discovered that a heap overflow in the AWT FileDialog.show() method could allow an attacker to cause a denial of service through an application crash or possibly execute arbitrary code. (CVE-2011-0815)

It was dicovered that integer overflows in the JPEGImageReader readImage() function and the SunLayoutEngine nativeLayout() function could allow an attacker to cause a denial of service through an application crash or possibly execute arbitrary code. (CVE-2011-0822, CVE-2011-0862)

It was discovered that memory corruption could occur when interpreting bytecode in the HotSpot VM. This could allow an attacker to cause a denial of service through an application crash or possibly execute arbitrary code. (CVE-2011-0864)

It was discovered that the deserialization code allowed the creation of mutable SignedObjects. This could allow an attacker to possibly execute code with elevated privileges. (CVE-2011-0865)

It was discovered that the toString method in the NetworkInterface class would reveal multiple addresses if they were bound to the interface. This could give an attacker more information about the networking environment. (CVE-2011-0867)

It was discovered that the Java 2D code to transform an image with a scale close to 0 could trigger an integer overflow. This could allow an attacker to cause a denial of service through an application crash or possibly execute arbitrary code. (CVE-2011-0868)

It was discovered that the SOAP with Attachments API for Java (SAAJ) implementation allowed the modification of proxy settings via unprivileged SOAP messages. (CVE-2011-0869, CVE-2011-0870)

It was the discovered that the Swing ImageIcon class created MediaTracker objects that potentially leaked privileged

ApplicationContexts. This could possibly allow an attacker access to restricted resources or services. (CVE-2011-0871)

It was discovered that non-blocking sockets marked as not urgent could still get selected for read operations. This could allow an attacker to cause a denial of service. (CVE-2011-0872)

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1154-1/

Risk Factor

Critical/ CVSS Base Score: 10.0
(CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVE

CVE-2011-0815
CVE-2011-0822
CVE-2011-0862
CVE-2011-0864
CVE-2011-0865
CVE-2011-0867
CVE-2011-0868
CVE-2011-0869
CVE-2011-0870
CVE-2011-0871
CVE-2011-0872

Other references

IAVA:2011-A-0102
IAVA:2011-A-0104
USN:1154-1

Patch publication date: 2011/06/17
Plugin publication date: 2011/06/20

Plugin last modification date: 2011/12/12

Port cifs (445/tcp)

Plugin ID: 10860
SMB Use Host SID to Enumerate Local Users

Synopsis

It is possible to enumerate local users.
List of Hosts

192.168.0.67
Plugin Output

- Administrator (id 500, Administrator account)
- nobody (id 501, Guest account)
- root (id 1000)
- root (id 1001)
- daemon (id 1002)
- daemon (id 1003)
- bin (id 1004)
- bin (id 1005)
- sys (id 1006)
- sys (id 1007)
- sync (id 1008)
- adm (id 1009)
- games (id 1010)
- tty (id 1011)
- man (id 1012)
- disk (id 1013)
- lp (id 1014)
- lp (id 1015)
- mail (id 1016)
- mail (id 1017)
- news (id 1018)
- news (id 1019)
- uucp (id 1020)
- uucp (id 1021)
- man (id 1025)
- proxy (id 1026)

- proxy (id 1027)
- kmem (id 1031)
- dialout (id 1041)
- fax (id 1043)
- voice (id 1045)
- cdrom (id 1049)
- floppy (id 1051)
- tape (id 1053)
- sudo (id 1055)
- audio (id 1059)
- dip (id 1061)
- www-data (id 1066)
- www-data (id 1067)
- backup (id 1068)
- backup (id 1069)
- operator (id 1075)
- list (id 1076)
- list (id 1077)
- irc (id 1078)
- irc (id 1079)
- src (id 1081)
- gnats (id 1082)
- gnats (id 1083)
- shadow (id 1085)
- utmp (id 1087)
- video (id 1089)
- sasl (id 1091)
- plugdev (id 1093)
- staff (id 1101)
- games (id 1121)
- libuuid (id 1200)

Note that, in addition to the Administrator and Guest accounts, Nessus has enumerated only those local users with IDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Start UID' and/or 'End UID' preferences for this plugin, then re-run the scan.

192.168.0.59
Plugin Output

- nobody (id 501, Guest account)

Note that, in addition to the Administrator and Guest accounts, Nessus has enumerated only those local users with IDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Start UID' and/or 'End UID' preferences for this plugin, then re-run the scan.

192.168.0.54
Plugin Output

- nobody (id 501, Guest account)

Note that, in addition to the Administrator and Guest accounts, Nessus has enumerated only those local users with IDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Start UID' and/or 'End UID' preferences for this plugin, then re-run the scan.

192.168.0.53
Plugin Output

- nobody (id 501, Guest account)

Note that, in addition to the Administrator and Guest accounts, Nessus has enumerated only those local users with IDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Start UID' and/or 'End UID' preferences for this plugin, then re-run the scan.

192.168.0.52
Plugin Output

- nobody (id 501, Guest account)

Note that, in addition to the Administrator and Guest accounts, Nessus has enumerated only those local users with IDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Start UID' and/or 'End UID' preferences for this plugin, then re-run the scan.

192.168.0.41
Plugin Output

- nobody (id 501, Guest account)

Note that, in addition to the Administrator and Guest accounts, Nessus has enumerated only those local users with IDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Start UID' and/or 'End UID' preferences for this plugin, then re-run the scan.

192.168.0.33
Plugin Output

- nobody (id 501, Guest account)

Note that, in addition to the Administrator and Guest accounts, Nessus has enumerated only those local users with IDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Start UID' and/or 'End UID' preferences for this plugin, then re-run the scan.

192.168.0.25
Plugin Output

- nobody (id 501, Guest account)

Note that, in addition to the Administrator and Guest accounts, Nessus has enumerated only those local users with IDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Start UID' and/or 'End UID' preferences for this plugin, then re-run the scan.

192.168.0.24
Plugin Output

- nobody (id 501, Guest account)

Note that, in addition to the Administrator and Guest accounts, Nessus has enumerated only those local users with IDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Start UID' and/or 'End UID' preferences for this plugin, then re-run the scan.

192.168.0.21
Plugin Output

- nobody (id 501, Guest account)
- root (id 1000)
- daemon (id 1002)
- bin (id 1004)
- sys (id 1006)
- sync (id 1008)
- games (id 1010)
- man (id 1012)
- lp (id 1014)
- mail (id 1016)
- news (id 1018)
- uucp (id 1020)
- proxy (id 1026)
- www-data (id 1066)
- backup (id 1068)

- list (id 1076)
- irc (id 1078)
- gnats (id 1082)
- dhcp (id 1200)

Note that, in addition to the Administrator and Guest accounts, Nessus has enumerated only those local users with IDs between 1000 and 1200. To use a different range, edit the scan policy and change the 'Start UID' and/or 'End UID' preferences for this plugin, then re-run the scan.

Description
Using the host security identifier (SID), it is possible to enumerate local users on the remote Windows system.

Solution
n/a

Risk Factor
None

Vulnerability publication date: 1998/04/28
Plugin publication date: 2002/02/13
Plugin last modification date: 2011/09/15

Ease of exploitability: Exploits are available

Port (0/tcp)

Plugin ID: 55101
USN-1139-1 : bind9 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

List of Hosts

192.168.0.25

Plugin Output

- Installed package : libdns64_1:9.7.0.dfsg.P1-1ubuntu0.1
Fixed package : libdns64_1:9.7.0.dfsg.P1-1ubuntu0.2

Description

It was discovered that Bind incorrectly handled certain bad signatures if multiple trust anchors existed for a single zone. A remote attacker could use this flaw to cause Bind to stop responding, resulting in a denial of service. This issue only affected Ubuntu 8.04 LTS and 10.04 LTS. (CVE-2010-3762)

Frank Kloeker and Michael Sinatra discovered that Bind incorrectly handled certain very large RRSIG RRsets included in negative responses. A remote attacker could use this flaw to cause Bind to stop responding, resulting in a denial of service. (CVE-2011-1910)

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1139-1/

Risk Factor

Medium/ CVSS Base Score: 5.0
(CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVE

CVE-2010-3762
CVE-2011-1910

Other references
USN:1139-1

Patch publication date: 2011/05/30
Plugin publication date: 2011/06/13

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 57449
USN-1320-1 : ffmpeg vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : libavformat52_4:0.5.1-1ubuntu1.1
Fixed package : libavformat52_4:0.5.1-1ubuntu1.3

Description
Steve Manzuik discovered that FFmpeg incorrectly handled certain malformed Matroska files. If a user were tricked into opening a crafted Matroska file, an attacker could cause a denial of service via application crash, or possibly execute arbitrary code with the privileges of the user invoking the program. (CVE-2011-3504)

Phillip Langlois discovered that FFmpeg incorrectly handled certain malformed QDM2 streams. If a user were tricked into opening a crafted QDM2 stream file, an attacker could cause a denial of service via

application crash, or possibly execute arbitrary code with the privileges of the user invoking the program. (CVE-2011-4351)

Phillip Langlois discovered that FFmpeg incorrectly handled certain malformed VP3 streams. If a user were tricked into opening a crafted file, an attacker could cause a denial of service via application crash, or possibly execute arbitrary code with the privileges of the user invoking the program. This issue only affected Ubuntu 10.10. (CVE-2011-4352)

Phillip Langlois discovered that FFmpeg incorrectly handled certain malformed VP5 and VP6 streams. If a user were tricked into opening a crafted file, an attacker could cause a denial of service via application crash, or possibly execute arbitrary code with the privileges of the user invoking the program. (CVE-2011-4353)

It was discovered that FFmpeg incorrectly handled certain malformed VMD files. If a user were tricked into opening a crafted VMD file, an attacker could cause a denial of service via application crash, or possibly execute arbitrary code with the privileges of the user invoking the program. (CVE-2011-4364)

Phillip Langlois discovered that FFmpeg incorrectly handled certain malformed SVQ1 streams. If a user were tricked into opening a crafted SVQ1 stream file, an attacker could cause a denial of service via application crash, or possibly execute arbitrary code with the privileges of the user invoking the program. (CVE-2011-4579)

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1320-1/

Risk Factor

High/ CVSS Base Score: 9.3
(CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVE
CVE-2011-3504
CVE-2011-4351
CVE-2011-4352
CVE-2011-4353
CVE-2011-4364
CVE-2011-4579

Other references
USN:1320-1

Patch publication date: 2012/01/05
Plugin publication date: 2012/01/06

Plugin last modification date: 2012/01/06

Port cifs (445/tcp)

Plugin ID: 26919
Microsoft Windows SMB Guest Account Local User Access

Synopsis

It is possible to log into the remote host.
List of Hosts

192.168.0.59

192.168.0.54

192.168.0.53

192.168.0.52

192.168.0.41

192.168.0.33

192.168.0.25

192.168.0.24

Description
The remote host is running one of the Microsoft Windows operating systems. It was possible to log into it as a guest user using a random account.

Solution
In the group policy change the setting for 'Network access: Sharing and security model for local accounts' from 'Guest only - local users authenticate as Guest' to 'Classic - local users authenticate as themselves'.

Risk Factor
Medium/ CVSS Base Score: 5.0
(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVE
CVE-1999-0505

Plugin publication date: 2007/10/04

Plugin last modification date: 2011/03/21

Port (0/tcp)

Plugin ID: 56089
USN-1197-2 : thunderbird vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25

Plugin Output

- Installed package : thunderbird_3.1.10+build1+nobinonly-0ubuntu0.10.04.1
Fixed package : thunderbird_3.1.13+build1+nobinonly-0ubuntu0.10.04.1

Description

USN-1197-1 fixed a vulnerability in Firefox with regard to the DigiNotar certificate authority. This update provides the corresponding updates for Thunderbird.

We are aware that the DigiNotar Root CA Certificate is still shown as trusted in the Thunderbird certificate manager. This is due to Thunderbird using the system version of the Network Security Service libraries (NSS). Thunderbird will actively distrust any certificate signed by this DigiNotar Root CA certificate. This means that users will still get an untrusted certificate warning when accessing a service through Thunderbird that presents a certificate signed by this DigiNotar Root CA certificate.

Original advisory details:

It was discovered that Dutch Certificate Authority DigiNotar had mis-issued multiple fraudulent certificates. These certificates could allow an attacker to perform a 'man in the middle' (MITM) attack which would make the user believe their connection is secure, but is actually being monitored.

For the protection of its users, Mozilla has removed the DigiNotar certificate. Sites using certificates issued by DigiNotar will need to seek another certificate vendor.

We are currently aware of a regression that blocks one of two Staat der Nederlanden root certificates which are believed to still be secure. This regression is being tracked at https://launchpad.net/bugs/838322.

Solution

Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1197-2/

Risk Factor
High

Other references
USN:1197-2

Patch publication date: 2011/09/02
Plugin publication date: 2011/09/06

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 56048
USN-1199-1 : apache2 vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : apache2.2-bin_2.2.14-5ubuntu8.4
Fixed package : apache2.2-bin_2.2.14-5ubuntu8.6

Description

A flaw was discovered in the byterange filter in Apache. A remote attacker could exploit this to cause a denial of service via resource exhaustion.

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1199-1/

Risk Factor
Medium/ CVSS Base Score: 5.0
(CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVE
CVE-2011-3192

Other references
IAVA:2011-A-0120
USN:1199-1

Patch publication date: 2011/09/01
Plugin publication date: 2011/09/02

Plugin last modification date: 2011/12/12

Port cifs (445/tcp)

Plugin ID: 25240
Samba Server Detection

Synopsis

An SMB server is running on the remote host.

List of Hosts

192.168.0.67

192.168.0.59

192.168.0.54

192.168.0.53

192.168.0.52

192.168.0.41

192.168.0.33

192.168.0.25

192.168.0.24

192.168.0.21

Description

The remote host is running Samba, a CIFS/SMB server for Linux and Unix.

Solution

n/a

See also

http://www.samba.org/

Risk Factor

None

Plugin publication date: 2007/05/16

Plugin last modification date: 2011/09/14

Port www (80/tcp)

Plugin ID: 40984
Browsable Web Directories

Synopsis

Some directories on the remote web server are browsable.
List of Hosts

192.168.0.40
Plugin Output

The following directories are browsable :

http://192.168.0.40/xp/
http://192.168.0.40/ubuntu/
http://192.168.0.40/

192.168.0.21
Plugin Output

The following directories are browsable :

http://192.168.0.21/php/

Description
Miscellaneous Nessus plugins identified directories on this web server that are browsable.

Solution
Make sure that browsable directories do not leak confidential informative or give access to sensitive resources. And use access

restrictions or disable directory indexing for any that do.

See also
http://projects.webappsec.org/Directory-Indexing

Risk Factor
None

Plugin publication date: 2009/09/15

Plugin last modification date: 2011/04/29

Port cifs (445/tcp)

Plugin ID: 10859
Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration

---

Synopsis

It is possible to obtain the host SID for the remote host.
List of Hosts

192.168.0.67
Plugin Output

The remote host SID value is :

1-5-21-1042354039-2475377354-766472396

The value of 'RestrictAnonymous' setting is : unknown

192.168.0.59
Plugin Output

The remote host SID value is :

1-5-21-666894502-544542872-3755517494

The value of 'RestrictAnonymous' setting is : unknown

192.168.0.54
Plugin Output

The remote host SID value is :

1-5-21-2147485045-1270253367-3880790715

The value of 'RestrictAnonymous' setting is : unknown

192.168.0.53
Plugin Output

The remote host SID value is :

1-5-21-4027264174-2180206719-1324994142

The value of 'RestrictAnonymous' setting is : unknown

192.168.0.52
Plugin Output

The remote host SID value is :

1-5-21-1805027819-3151103239-3623397535

The value of 'RestrictAnonymous' setting is : unknown

192.168.0.41
Plugin Output

The remote host SID value is :

1-5-21-2927860511-2524574811-348447334

The value of 'RestrictAnonymous' setting is : unknown

192.168.0.33
Plugin Output

The remote host SID value is :

1-5-21-4001140026-2471097955-1588623547

The value of 'RestrictAnonymous' setting is : unknown

192.168.0.25
Plugin Output

The remote host SID value is :

1-5-21-3355021099-3275509345-1129450993

The value of 'RestrictAnonymous' setting is : unknown

192.168.0.24
Plugin Output

The remote host SID value is :

1-5-21-2122457733-456491822-2518509805

The value of 'RestrictAnonymous' setting is : unknown

192.168.0.21
Plugin Output

The remote host SID value is :

1-5-21-2952145021-507220021-499326276

The value of 'RestrictAnonymous' setting is : unknown

Description

By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier).

The host SID can then be used to get the list of local users.

Solution

You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value.

Refer to the 'See also' section for guidance.

See also

http://technet.microsoft.com/en-us/library/bb418944.aspx

Risk Factor
None

Vulnerability publication date: 2000/01/31
Plugin publication date: 2002/02/13
Plugin last modification date: 2011/09/15

Ease of exploitability: Exploits are available

Port netbios-ns (137/udp)

Plugin ID: 43815
NetBIOS Multiple IP Address Enumeration

Synopsis

The remote host is configured with multiple IP addresses.
List of Hosts

192.168.0.59
Plugin Output

The remote host appears to be using the following IP addresses :

- 192.168.43.1
- 172.16.227.1

192.168.0.54
Plugin Output

The remote host appears to be using the following IP addresses :

- 192.168.43.1
- 172.16.227.1

192.168.0.53
Plugin Output

The remote host appears to be using the following IP addresses :

- 192.168.0.53
- 192.168.43.1
- 172.16.227.1

192.168.0.52
Plugin Output

The remote host appears to be using the following IP addresses :

- 192.168.43.1
- 172.16.227.1

192.168.0.41
Plugin Output

The remote host appears to be using the following IP addresses :

- 192.168.43.1
- 172.16.227.1

192.168.0.33
Plugin Output

The remote host appears to be using the following IP addresses :

- 192.168.43.1
- 172.16.227.1

192.168.0.25
Plugin Output

The remote host appears to be using the following IP addresses :

- 192.168.43.1
- 172.16.227.1

192.168.0.24
Plugin Output

The remote host appears to be using the following IP addresses :

- 192.168.1.5
- 192.168.43.1
- 172.16.227.1

Description
By sending a special NetBIOS query, Nessus was able to detect the use of multiple IP addresses on the remote host. This indicates the host may be running virtualization software, a VPN client, or has multiple network interfaces.

Solution
n/a

Risk Factor
None

Plugin publication date: 2010/01/06

Plugin last modification date: 2011/09/02

Port netbios-ns (137/udp)

Plugin ID: 10150
Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

It is possible to obtain the network name of the remote host.
List of Hosts

192.168.0.67
Plugin Output
The following 7 NetBIOS names have been gathered :

METASPLOITABLE = Computer name
METASPLOITABLE = Messenger Service
METASPLOITABLE = File Server Service
__MSBROWSE__ = Master Browser
WORKGROUP = Workgroup / Domain name

WORKGROUP = Master Browser
WORKGROUP = Browser Service Elections

This SMB server seems to be a SAMBA server (MAC address is NULL).

192.168.0.59
Plugin Output
The following 7 NetBIOS names have been gathered :

BT = Computer name
BT = Messenger Service
BT = File Server Service
__MSBROWSE__ = Master Browser
WORKGROUP = Master Browser
WORKGROUP = Browser Service Elections
WORKGROUP = Workgroup / Domain name

This SMB server seems to be a SAMBA server (MAC address is NULL).

192.168.0.54
Plugin Output
The following 7 NetBIOS names have been gathered :

BT = Computer name
BT = Messenger Service
BT = File Server Service
__MSBROWSE__ = Master Browser
WORKGROUP = Master Browser
WORKGROUP = Browser Service Elections
WORKGROUP = Workgroup / Domain name

This SMB server seems to be a SAMBA server (MAC address is NULL).

192.168.0.53
Plugin Output
The following 7 NetBIOS names have been gathered :

BT = Computer name
BT = Messenger Service
BT = File Server Service
__MSBROWSE__ = Master Browser
WORKGROUP = Master Browser
WORKGROUP = Browser Service Elections
WORKGROUP = Workgroup / Domain name

This SMB server seems to be a SAMBA server (MAC address is NULL).

192.168.0.52

Plugin Output
The following 7 NetBIOS names have been gathered :

BT = Computer name
BT = Messenger Service
BT = File Server Service
__MSBROWSE__ = Master Browser
WORKGROUP = Master Browser
WORKGROUP = Browser Service Elections
WORKGROUP = Workgroup / Domain name

This SMB server seems to be a SAMBA server (MAC address is NULL).

192.168.0.41
Plugin Output
The following 7 NetBIOS names have been gathered :

BT = Computer name
BT = Messenger Service
BT = File Server Service
__MSBROWSE__ = Master Browser
WORKGROUP = Master Browser
WORKGROUP = Browser Service Elections
WORKGROUP = Workgroup / Domain name

This SMB server seems to be a SAMBA server (MAC address is NULL).

192.168.0.33
Plugin Output
The following 7 NetBIOS names have been gathered :

BT = Computer name
BT = Messenger Service
BT = File Server Service
__MSBROWSE__ = Master Browser
WORKGROUP = Master Browser
WORKGROUP = Browser Service Elections
WORKGROUP = Workgroup / Domain name

This SMB server seems to be a SAMBA server (MAC address is NULL).

192.168.0.25
Plugin Output
The following 7 NetBIOS names have been gathered :

BT = Computer name
BT = Messenger Service
BT = File Server Service

__MSBROWSE__ = Master Browser
WORKGROUP = Master Browser
WORKGROUP = Browser Service Elections
WORKGROUP = Workgroup / Domain name

This SMB server seems to be a SAMBA server (MAC address is NULL).

192.168.0.24
Plugin Output
The following 7 NetBIOS names have been gathered :

BT = Computer name
BT = Messenger Service
BT = File Server Service
__MSBROWSE__ = Master Browser
WORKGROUP = Master Browser
WORKGROUP = Browser Service Elections
WORKGROUP = Workgroup / Domain name

This SMB server seems to be a SAMBA server (MAC address is NULL).

192.168.0.21
Plugin Output
The following 7 NetBIOS names have been gathered :

UBUNTUVM = Computer name
UBUNTUVM = Messenger Service
UBUNTUVM = File Server Service
__MSBROWSE__ = Master Browser
MSHOME = Master Browser
MSHOME = Browser Service Elections
MSHOME = Workgroup / Domain name

This SMB server seems to be a SAMBA server (MAC address is NULL).

Description
The remote host listens on UDP port 137 or TCP port 445 and replies to
NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins
but does not itself generate a report.

Solution
n/a

Risk Factor
None

Plugin publication date: 1999/10/12

Plugin last modification date: 2011/05/24

Port (0/tcp)

Plugin ID: 55472
Device Hostname

Synopsis

It is possible to determine the remote system hostname.
List of Hosts

192.168.0.25
Plugin Output

Hostname : bt

Description
This plugin reports a device's hostname collected via SSH or WMI.

Solution
n/a

Risk Factor
None

Plugin publication date: 2011/06/30

Plugin last modification date: 2011/07/01

Port (0/tcp)

Plugin ID: 56860
USN-1263-1 : icedtea-web, openjdk-6, openjdk-6b18 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : icedtea-6-jre-cacao_6b20-1.9.7-0ubuntu1~10.04.1
Fixed package : icedtea-6-jre-cacao_6b20-1.9.10-0ubuntu1~10.04.2

- Installed package : openjdk-6-jre_6b20-1.9.7-0ubuntu1~10.04.1
Fixed package : openjdk-6-jre_6b20-1.9.10-0ubuntu1~10.04.2

- Installed package : openjdk-6-jre-headless_6b20-1.9.7-0ubuntu1~10.04.1
Fixed package : openjdk-6-jre-headless_6b20-1.9.10-0ubuntu1~10.04.2

- Installed package : openjdk-6-jre-lib_6b20-1.9.7-0ubuntu1~10.04.1
Fixed package : openjdk-6-jre-lib_6b20-1.9.10-0ubuntu1~10.04.2

Description
Deepak Bhole discovered a flaw in the Same Origin Policy (SOP) implementation in the IcedTea web browser plugin. This could allow a remote attacker to open connections to certain hosts that should not

be permitted. (CVE-2011-3377)

Juliano Rizzo and Thai Duong discovered that the block-wise AES encryption algorithm block-wise as used in TLS/SSL was vulnerable to a chosen-plaintext attack. This could allow a remote attacker to view confidential data. (CVE-2011-3389)

It was discovered that a type confusion flaw existed in the in the Internet Inter-Orb Protocol (IIOP) deserialization code. A remote attacker could use this to cause an untrusted application or applet to execute arbitrary code by deserializing malicious input. (CVE-2011-3521)

It was discovered that the Java scripting engine did not perform SecurityManager checks. This could allow a remote attacker to cause an untrusted application or applet to execute arbitrary code with the full privileges of the JVM. (CVE-2011-3544)

It was discovered that the InputStream class used a global buffer to store input bytes skipped. An attacker could possibly use this to gain access to sensitive information. (CVE-2011-3547)

It was discovered that a vulnerability existed in the AWTKeyStroke class. A remote attacker could cause an untrusted application or applet to execute arbitrary code. (CVE-2011-3548)

It was discovered that an integer overflow vulnerability existed in the TransformHelper class in the Java2D implementation. A remote attacker could use this cause a denial of service via an application or applet crash or possibly execute arbitrary code. (CVE-2011-3551)

It was discovered that the default number of available UDP sockets for applications running under SecurityManager restrictions was set too high. A remote attacker could use this with a malicious application or applet exhaust the number of available UDP sockets to cause a denial of service for other applets or applications running within the same JVM. (CVE-2011-3552)

It was discovered that Java API for XML Web Services (JAX-WS) could incorrectly expose a stack trace. A remote attacker could potentially use this to gain access to sensitive information. (CVE-2011-3553)

It was discovered that the unpacker for pack200 JAR files did not sufficiently check for errors. An attacker could cause a denial of service or possibly execute arbitrary code through a specially crafted pack200 JAR file. (CVE-2011-3554)

It was discovered that the RMI registration implementation did not

properly restrict privileges of remotely executed code. A remote attacker could use this to execute code with elevated privileges. (CVE-2011-3556, CVE-2011-3557)

It was discovered that the HotSpot VM could be made to crash, allowing an attacker to cause a denial of service or possibly leak sensitive information. (CVE-2011-3558)

It was discovered that the HttpsURLConnection class did not properly perform SecurityManager checks in certain situations. This could allow a remote attacker to bypass restrictions on HTTPS connections. (CVE-2011-3560)

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1263-1/

Risk Factor

Critical/ CVSS Base Score: 10.0
(CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVE

CVE-2011-3377
CVE-2011-3389
CVE-2011-3521
CVE-2011-3544
CVE-2011-3547
CVE-2011-3548
CVE-2011-3551
CVE-2011-3552
CVE-2011-3553
CVE-2011-3554
CVE-2011-3556
CVE-2011-3557
CVE-2011-3558
CVE-2011-3560

Other references
IAVA:2011-A-0142
IAVA:2012-A-0004
IAVA:2011-A-0155
USN:1263-1

Patch publication date: 2011/11/16
Plugin publication date: 2011/11/17
Plugin last modification date: 2012/01/15
Ease of exploitability: Exploits are available

Exploitable with: Canvas (CANVAS), Metasploit (Java Applet Rhino Script Engine Remote Code Execution)

Port ssh (22/tcp)

Plugin ID: 10267
SSH Server Type and Version Information

Synopsis

An SSH server is listening on this port.
List of Hosts

192.168.0.67
Plugin Output

SSH version : SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
SSH supported authentication : publickey,password

192.168.0.40
Plugin Output

SSH version : SSH-2.0-OpenSSH_5.5p1 Debian-4ubuntu6
SSH supported authentication : publickey,password

192.168.0.21
Plugin Output

SSH version : SSH-2.0-OpenSSH_4.6p1 Debian-5build1

SSH supported authentication : publickey,password

Description
It is possible to obtain information about the remote SSH
server by sending an empty authentication request.

Solution
n/a

Risk Factor
None

Plugin publication date: 1999/10/12

Plugin last modification date: 2011/10/24

Port (0/tcp)

Plugin ID: 11936
OS Identification

Synopsis

It is possible to guess the remote operating system.
List of Hosts

192.168.0.67
Plugin Output

Remote operating system : Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Confidence Level : 95
Method : SSH

The remote host is running Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

192.168.0.59
Plugin Output

Remote operating system : Linux Kernel 2.6
Confidence Level : 65
Method : SinFP

The remote host is running Linux Kernel 2.6

192.168.0.54
Plugin Output

Remote operating system : Linux Kernel 2.6
Confidence Level : 65
Method : SinFP

The remote host is running Linux Kernel 2.6

192.168.0.53
Plugin Output

Remote operating system : Linux Kernel 2.6
Confidence Level : 65
Method : SinFP

The remote host is running Linux Kernel 2.6

192.168.0.52
Plugin Output

Remote operating system : Linux Kernel 2.6
Confidence Level : 65
Method : SinFP

The remote host is running Linux Kernel 2.6

192.168.0.41
Plugin Output

Remote operating system : Linux Kernel 2.6
Confidence Level : 65
Method : SinFP

The remote host is running Linux Kernel 2.6

192.168.0.40
Plugin Output

Remote operating system : Linux Kernel 2.6 on Ubuntu 10.10 (maverick)
Confidence Level : 95
Method : SSH

The remote host is running Linux Kernel 2.6 on Ubuntu 10.10 (maverick)

192.168.0.33
Plugin Output

Remote operating system : Linux Kernel 2.6
Confidence Level : 65
Method : SinFP

The remote host is running Linux Kernel 2.6

192.168.0.25
Plugin Output

Remote operating system : Linux Kernel 2.6.39.4 on Ubuntu 10.04
Confidence Level : 100
Method : LinuxDistribution

The remote host is running Linux Kernel 2.6.39.4 on Ubuntu 10.04

192.168.0.24
Plugin Output

Remote operating system : Linux Kernel 2.6
Confidence Level : 65
Method : SinFP

The remote host is running Linux Kernel 2.6

192.168.0.23
Plugin Output

Remote operating system : Linux Kernel 2.6

Confidence Level : 65
Method : SinFP

The remote host is running Linux Kernel 2.6

192.168.0.21
Plugin Output

Remote operating system : Linux Kernel 2.6
Confidence Level : 70
Method : SinFP

The remote host is running Linux Kernel 2.6

Description
Using a combination of remote probes, (TCP/IP, SMB, HTTP, NTP, SNMP, etc...)
it is possible to guess the name of the remote operating system in use, and
sometimes its version.

Solution
N/A

Risk Factor
None

Plugin publication date: 2003/12/09

Plugin last modification date: 2012/01/09

Port cifs (445/tcp)

Plugin ID: 11011
Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

List of Hosts

192.168.0.67

Plugin Output

A CIFS server is running on this port.

192.168.0.59

Plugin Output

A CIFS server is running on this port.

192.168.0.54

Plugin Output

A CIFS server is running on this port.

192.168.0.53

Plugin Output

A CIFS server is running on this port.

192.168.0.52

Plugin Output

A CIFS server is running on this port.

192.168.0.41

Plugin Output

A CIFS server is running on this port.

192.168.0.33

Plugin Output

A CIFS server is running on this port.

192.168.0.25

Plugin Output

A CIFS server is running on this port.

192.168.0.24

Plugin Output

A CIFS server is running on this port.

192.168.0.21
Plugin Output

A CIFS server is running on this port.

Description
The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution
n/a

Risk Factor
None

Plugin publication date: 2002/06/05

Plugin last modification date: 2011/03/11

Port smb (139/tcp)

Plugin ID: 11011
Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.
List of Hosts

192.168.0.67
Plugin Output

An SMB server is running on this port.

192.168.0.59
Plugin Output

An SMB server is running on this port.

192.168.0.54
Plugin Output

An SMB server is running on this port.

192.168.0.53
Plugin Output

An SMB server is running on this port.

192.168.0.52
Plugin Output

An SMB server is running on this port.

192.168.0.41
Plugin Output

An SMB server is running on this port.

192.168.0.33
Plugin Output

An SMB server is running on this port.

192.168.0.25
Plugin Output

An SMB server is running on this port.

192.168.0.24
Plugin Output

An SMB server is running on this port.

192.168.0.21
Plugin Output

An SMB server is running on this port.

Description
The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution
n/a

Risk Factor
None

Plugin publication date: 2002/06/05

Plugin last modification date: 2011/03/11

Port ajp13 (8009/tcp)

Plugin ID: 21186
AJP Connector Detection

Synopsis

There is an AJP connector listening on the remote host.
List of Hosts

192.168.0.67
Plugin Output

The connector listing on this port supports the ajp13 protocol.

Description
The remote host is running an AJP (Apache JServ Protocol) connector, a service by which a standalone web server such as Apache communicates over TCP with a Java servlet container such as Tomcat.

Solution
n/a

See also
http://tomcat.apache.org/connectors-doc/
http://tomcat.apache.org/connectors-doc/ajp/ajpv13a.html

Risk Factor
None

Plugin publication date: 2006/04/05

Plugin last modification date: 2011/03/11

Port www (8834/tcp)

Plugin ID: 21643
SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.
List of Hosts

192.168.0.59
Plugin Output

Here is the list of SSL ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)
SSLv3
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
TLSv1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
AES128-SHA Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

192.168.0.54
Plugin Output

Here is the list of SSL ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)
SSLv3
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
TLSv1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
AES128-SHA Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

192.168.0.53
Plugin Output

Here is the list of SSL ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)
SSLv3
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
TLSv1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
AES128-SHA Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

192.168.0.52
Plugin Output

Here is the list of SSL ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)
SSLv3
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
TLSv1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
AES128-SHA Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}

Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

192.168.0.41
Plugin Output

Here is the list of SSL ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)
SSLv3
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
TLSv1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
AES128-SHA Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

192.168.0.33
Plugin Output

Here is the list of SSL ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)
SSLv3
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
TLSv1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
AES128-SHA Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

192.168.0.25
Plugin Output

Here is the list of SSL ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)
SSLv3
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
TLSv1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
AES128-SHA Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

192.168.0.24
Plugin Output

Here is the list of SSL ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)
SSLv3
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1
TLSv1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
AES128-SHA Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1

RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

Description
This script detects which SSL ciphers are supported by the remote service for encrypting communications.

Solution
n/a

See also
http://www.openssl.org/docs/apps/ciphers.html

Risk Factor
None

Plugin publication date: 2006/06/05

Plugin last modification date: 2012/01/23

Port nessus (1241/tcp)

Plugin ID: 21643

SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

List of Hosts

192.168.0.59

Plugin Output

Here is the list of SSL ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)
TLSv1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
AES128-SHA Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

192.168.0.54

Plugin Output

Here is the list of SSL ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)
TLSv1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
AES128-SHA Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}

Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

192.168.0.53
Plugin Output

Here is the list of SSL ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)
TLSv1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
AES128-SHA Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

192.168.0.52
Plugin Output

Here is the list of SSL ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)
TLSv1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
AES128-SHA Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

192.168.0.41
Plugin Output

Here is the list of SSL ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)
TLSv1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
AES128-SHA Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

192.168.0.33
Plugin Output

Here is the list of SSL ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)
TLSv1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
AES128-SHA Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

192.168.0.25
Plugin Output

Here is the list of SSL ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)
TLSv1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
AES128-SHA Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

192.168.0.24
Plugin Output

Here is the list of SSL ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)
TLSv1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
AES128-SHA Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
AES256-SHA Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

Description
This script detects which SSL ciphers are supported by the remote
service for encrypting communications.

Solution
n/a

See also
http://www.openssl.org/docs/apps/ciphers.html

Risk Factor
None

Plugin publication date: 2006/06/05

Plugin last modification date: 2012/01/23

Port (0/tcp)

Plugin ID: 56115
USN-1197-3 : firefox, xulrunner-1.9.2 vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : xulrunner-1.9.2_1.9.2.17+build3+nobinonly-0ubuntu0.10.04.1
Fixed package : xulrunner-1.9.2_1.9.2.22+build2+nobinonly-0ubuntu0.10.04.1

Description
USN-1197-1 partially addressed an issue with Dutch Certificate

Authority DigiNotar mis-issuing fraudulent certificates. This update actively distrusts the DigiNotar root certificate as well as several intermediary certificates. Also included in this list of distrusted certificates are the Staat der Nederlanden root certificates.

Original advisory details:

It was discovered that Dutch Certificate Authority DigiNotar, had mis-issued multiple fraudulent certificates. These certificates could allow an attacker to perform a 'man in the middle' (MITM) attack which would make the user believe their connection is secure, but is actually being monitored.

For the protection of its users, Mozilla has removed the DigiNotar certificate. Sites using certificates issued by DigiNotar will need to seek another certificate vendor.

We are currently aware of a regression that blocks one of two Staat der Nederlanden root certificates which are believed to still be secure. This regression is being tracked at https://launchpad.net/bugs/838322.

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1197-3/

Risk Factor

High

Other references

USN:1197-3

Patch publication date: 2011/09/07
Plugin publication date: 2011/09/07

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 57314
USN-1307-1 : php5 vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : php5-cgi_5.3.2-1ubuntu4.9
Fixed package : php5-cgi_5.3.2-1ubuntu4.11

- Installed package : php5-cli_5.3.2-1ubuntu4.9
Fixed package : php5-cli_5.3.2-1ubuntu4.11

Description
Florent Hochwelker discovered that PHP incorrectly handled certain
EXIF headers in JPEG files. A remote attacker could exploit this
issue to view sensitive information or cause the PHP server to crash.

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1307-1/

Risk Factor
Medium/ CVSS Base Score: 6.4
(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:P)

CVE
CVE-2011-4566

Other references
USN:1307-1

Patch publication date: 2011/12/14
Plugin publication date: 2011/12/15

Plugin last modification date: 2011/12/15

Port (0/tcp)

Plugin ID: 56206
USN-1207-1 : cups, cupsys vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : libcupsimage2_1.4.3-1ubuntu1.4
Fixed package : libcupsimage2_1.4.3-1ubuntu1.5

Description
Tomas Hoger discovered that the CUPS image library incorrectly handled LZW streams. A remote attacker could use this flaw to cause a denial of service or possibly execute arbitrary code.

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1207-1/

Risk Factor
Medium/ CVSS Base Score: 5.1
(CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVE
CVE-2011-2896
CVE-2011-3170

Other references
USN:1207-1

Patch publication date: 2011/09/14
Plugin publication date: 2011/09/15

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 25203
Enumerate IPv4 Interfaces via SSH

Synopsis

This plugin enumerates IPv4 interfaces on a remote host.
List of Hosts

192.168.0.25
Plugin Output

The following IPv4 addresses are set on the remote host :

- 192.168.0.25 (on interface eth0)
- 127.0.0.1 (on interface lo)
- 192.168.43.1 (on interface vmnet1)
- 172.16.227.1 (on interface vmnet8)

Description
By connecting to the remote host via SSH with the supplied credentials, this plugin enumerates network interfaces configured with IPv4 addresses.

Solution
Disable any unused IPv4 interfaces.

Risk Factor
None

Plugin publication date: 2007/05/11

Plugin last modification date: 2011/03/21

Port (0/tcp)

Plugin ID: 35716
Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be deduced from the Ethernet OUI.

List of Hosts

192.168.0.67

Plugin Output

The following card manufacturers were identified :

08:00:27:b3:f9:f8 : CADMUS COMPUTER SYSTEMS

192.168.0.63

Plugin Output

The following card manufacturers were identified :

08:00:27:a2:a6:32 : CADMUS COMPUTER SYSTEMS

192.168.0.59

Plugin Output

The following card manufacturers were identified :

00:26:2d:91:45:56 : Wistron Corporation

192.168.0.54

Plugin Output

The following card manufacturers were identified :

14:da:e9:23:0b:a4 : ASUSTek COMPUTER INC.

192.168.0.53

Plugin Output

The following card manufacturers were identified :

20:6a:8a:40:45:c8 : Wistron InfoComm Manufacturing(Kunshan)Co.,Ltd.

192.168.0.52

Plugin Output

The following card manufacturers were identified :

00:26:22:52:5f:c9 : COMPAL INFORMATION (KUNSHAN) CO., LTD.

192.168.0.41
Plugin Output

The following card manufacturers were identified :

00:23:8b:78:80:4f : Quanta Computer Inc.

192.168.0.40
Plugin Output

The following card manufacturers were identified :

10:78:d2:36:65:a4 : ELITEGROUP COMPUTER SYSTEM CO., LTD.

192.168.0.33
Plugin Output

The following card manufacturers were identified :

00:25:64:67:3b:1d : Dell Inc.

192.168.0.25
Plugin Output

The following card manufacturers were identified :

20:6a:8a:00:36:f2 : Wistron InfoComm Manufacturing(Kunshan)Co.,Ltd.
78:e4:00:f8:53:a7 : Hon Hai Precision Ind. Co.,Ltd.

192.168.0.24
Plugin Output

The following card manufacturers were identified :

00:26:22:73:84:f3 : COMPAL INFORMATION (KUNSHAN) CO., LTD.

192.168.0.23
Plugin Output

The following card manufacturers were identified :

98:4b:e1:c0:e6:b1 : Hewlett-Packard Company

192.168.0.21
Plugin Output

The following card manufacturers were identified :

08:00:27:f9:c1:bb : CADMUS COMPUTER SYSTEMS

Description
Each ethernet MAC address starts with a 24-bit 'Organizationally
Unique Identifier'.
These OUI are registered by IEEE.

Solution
n/a

See also
http://standards.ieee.org/faqs/OUI.html
http://standards.ieee.org/regauth/oui/index.shtml

Risk Factor
None

Plugin publication date: 2009/02/19

Plugin last modification date: 2011/03/27

Port (0/tcp)

Plugin ID: 57341
USN-1310-1 : libarchive vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : libarchive1_2.8.0-2
Fixed package : libarchive1_2.8.0-2ubuntu0.1

Description
It was discovered that libarchive incorrectly handled certain ISO 9660 image files. If a user were tricked into using a specially crafted ISO 9660 image file, a remote attacker could cause libarchive to crash or possibly execute arbitrary code with user privileges. (CVE-2011-1777)

It was discovered that libarchive incorrectly handled certain tar archive files. If a user were tricked into using a specially crafted tar file, a remote attacker could cause libarchive to crash or possibly execute arbitrary code with user privileges. (CVE-2011-1778)

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1310-1/

Risk Factor
High

CVE
CVE-2011-1777
CVE-2011-1778

Other references
USN:1310-1

Patch publication date: 2011/12/19
Plugin publication date: 2011/12/20

Plugin last modification date: 2011/12/20

Port (0/tcp)

Plugin ID: 56778
USN-1259-1 : apache2, apache2-mpm-itk vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : apache2.2-bin_2.2.14-5ubuntu8.4
Fixed package : apache2.2-bin_2.2.14-5ubuntu8.7

Description
It was discovered that the mod_proxy module in Apache did not properly interact with the RewriteRule and ProxyPassMatch pattern matches in the configuration of a reverse proxy. This could allow remote attackers to contact internal webservers behind the proxy that were not intended for external exposure. (CVE-2011-3368)

Stefano Nichele discovered that the mod_proxy_ajp module in Apache when used with mod_proxy_balancer in certain configurations could allow remote attackers to cause a denial of service via a malformed HTTP request. (CVE-2011-3348)

Samuel Montosa discovered that the ITK Multi-Processing Module for Apache did not properly handle certain configuration sections that specify NiceValue but not AssignUserID, preventing Apache from

dropping privileges correctly. This issue only affected Ubuntu 10.04 LTS, Ubuntu 10.10 and Ubuntu 11.04. (CVE-2011-1176)

USN 1199-1 fixed a vulnerability in the byterange filter of Apache. The upstream patch introduced a regression in Apache when handling specific byte range requests. This update fixes the issue.

Original advisory details:

A flaw was discovered in the byterange filter in Apache. A remote attacker could exploit this to cause a denial of service via resource exhaustion.

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1259-1/

Risk Factor
Medium/ CVSS Base Score: 5.0
(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

CVE
CVE-2011-1176
CVE-2011-3348
CVE-2011-3368

Other references
USN:1259-1

Patch publication date: 2011/11/11
Plugin publication date: 2011/11/11

Plugin last modification date: 2011/11/11

Port (0/tcp)

Plugin ID: 55531
USN-1165-1 : qemu-kvm vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

List of Hosts

192.168.0.25

Plugin Output

- Installed package : qemu-kvm_0.12.3+noroms-0ubuntu9.6
Fixed package : qemu-kvm_0.12.3+noroms-0ubuntu9.12

Description

Nelson Elhage discoverd that QEMU did not properly validate certain virtqueue requests from the guest. An attacker could exploit this to cause a denial of service of the guest or possibly execute code with the privileges of the user invoking the program. (CVE-2011-2212)

Stefan Hajnoczi discovered that QEMU did not properly perform integer comparisons when performing virtqueue input validation. An attacker could exploit this to cause a denial of service of the guest or possibly execute code with the privileges of the user invoking the program. (CVE-2011-2512)

When using QEMU with libvirt or virtualization management software based on libvirt such as Eucalyptus and OpenStack, QEMU guests are individually isolated by an AppArmor profile by default in Ubuntu.

Solution

Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1165-1/

Risk Factor
High

CVE
CVE-2011-2212
CVE-2011-2512

Other references
USN:1165-1

Patch publication date: 2011/07/06
Plugin publication date: 2011/07/07

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 56280
USN-1214-1 : gimp vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : gimp_2.6.8-2ubuntu1.2
Fixed package : gimp_2.6.8-2ubuntu1.4

Description

Tomas Hoger discovered that GIMP incorrectly handled malformed LZW streams. If a user were tricked into opening a specially crafted GIF image file, an attacker could cause GIMP to crash, or possibly execute arbitrary code with the user's privileges.

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1214-1/

Risk Factor

Medium/ CVSS Base Score: 5.1
(CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

CVE

CVE-2011-2896

Other references

USN:1214-1

Patch publication date: 2011/09/22
Plugin publication date: 2011/09/23

Plugin last modification date: 2011/10/21

Port vmware_auth (902/tcp)

Plugin ID: 20301
VMware ESX/GSX Server detection

Synopsis

The remote host appears to be running VMware Server, ESX Server, or GSX Server.
List of Hosts

192.168.0.59

192.168.0.54

192.168.0.53

192.168.0.52

192.168.0.41

192.168.0.33

192.168.0.25

192.168.0.24

Description
According to its banner, the remote host appears to be running a VMware server authentication daemon, which likely indicates the remote host is running VMware Server, ESX Server, or GSX Server.

Solution
n/a

See also
http://www.vmware.com/

Risk Factor
None

Plugin publication date: 2005/12/14

Plugin last modification date: 2011/11/28

Port (0/tcp)

Plugin ID: 57315
USN-1308-1 : bzip2 vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : bzip2_1.0.5-4ubuntu0.1
Fixed package : bzip2_1.0.5-4ubuntu0.2

Description
vladz discovered that executables compressed by bzexe insecurely
create temporary files when they are ran. A local attacker could
exploit this issue to execute arbitrary code as the user running a
compressed executable.

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1308-1/

Risk Factor
High

CVE
CVE-2011-4089

Other references
USN:1308-1

Patch publication date: 2011/12/14
Plugin publication date: 2011/12/15

Plugin last modification date: 2011/12/15

Port www (8834/tcp)

Plugin ID: 20108
Web Server / Application favicon.ico Vendor Fingerprinting

Synopsis

The remote web server contains a graphic image that is prone to information disclosure.
List of Hosts

192.168.0.59
Plugin Output

The MD5 fingerprint for 'favicon.ico' suggests the web server is Nessus 4.x Web Client.

192.168.0.54

Plugin Output

The MD5 fingerprint for 'favicon.ico' suggests the web server is Nessus 4.x Web Client.

192.168.0.53
Plugin Output

The MD5 fingerprint for 'favicon.ico' suggests the web server is Nessus 4.x Web Client.

192.168.0.52
Plugin Output

The MD5 fingerprint for 'favicon.ico' suggests the web server is Nessus 4.x Web Client.

192.168.0.41
Plugin Output

The MD5 fingerprint for 'favicon.ico' suggests the web server is Nessus 4.x Web Client.

192.168.0.33
Plugin Output

The MD5 fingerprint for 'favicon.ico' suggests the web server is Nessus 4.x Web Client.

192.168.0.25
Plugin Output

The MD5 fingerprint for 'favicon.ico' suggests the web server is Nessus 4.x Web Client.

192.168.0.24
Plugin Output

The MD5 fingerprint for 'favicon.ico' suggests the web server is Nessus 4.x Web Client.

Description
The 'favicon.ico' file found on the remote web server belongs to a
popular webserver. This may be used to fingerprint the web server.

Solution
Remove the 'favicon.ico' file or create a custom one for your site.

Risk Factor
None

Other references
OSVDB:39272

Plugin publication date: 2005/10/28

Plugin last modification date: 2011/11/01

Port www (80/tcp)

Plugin ID: 11419
Web Server Office File Inventory

Synopsis

The remote web server hosts office-related files.
List of Hosts

192.168.0.40
Plugin Output

The following office-related files are available on the remote server :

- Adobe Acrobat files (.pdf) :
/uu-ite-11-2008.pdf
/KitabUndang-undangHukumPidana_KUHP.pdf
/KitabUndang-undangHukumAcaraPidana_KUHAP.pdf

Description
This plugin connects to the remote web server and attempts to find
office-related files such as .doc, .ppt, .xls, .pdf etc.

Solution
Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

Risk Factor
None

Plugin publication date: 2003/03/19

Plugin last modification date: 2011/12/28

Port (0/tcp)

Plugin ID: 55717
USN-1177-1 : qemu-kvm vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : qemu-kvm_0.12.3+noroms-0ubuntu9.6
Fixed package : qemu-kvm_0.12.3+noroms-0ubuntu9.15

Description
Andrew Griffiths discovered that QEMU did not correctly drop privileges when using the 'runas' argument. Under certain circumstances a local attacker could exploit this to escalate privileges.

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1177-1/

Risk Factor
High

CVE
CVE-2011-2527

Other references
USN:1177-1

Patch publication date: 2011/07/27
Plugin publication date: 2011/07/28

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 55700
USN-1176-1 : dbus vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : dbus_1.2.16-2ubuntu4.2
Fixed package : dbus_1.2.16-2ubuntu4.3

Description
It was discovered that DBus did not properly validate the byte order of messages under certain circumstances. An attacker could exploit this to cause a denial of service via application crash or potentially obtain access to sensitive information.

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1176-1/

Risk Factor
Medium/ CVSS Base Score: 4.6
(CVSS2#AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVE
CVE-2011-2200

Other references
USN:1176-1

Patch publication date: 2011/07/26
Plugin publication date: 2011/07/27

Plugin last modification date: 2011/10/21

Port www (8834/tcp)

Plugin ID: 51192
SSL Certificate signed with an unknown Certificate Authority

Synopsis

The SSL certificate for this service is signed by an unknown certificate authority.
List of Hosts

192.168.0.59
Plugin Output

The following certificates were at the top of the certificate
chain sent by the remote host, but are signed by an unknown
certificate authority :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New
York/C=US/ST=NY/CN=Nessus Certification Authority
|-Issuer : O=Nessus Users United/OU=Nessus Certification Authority/L=New
York/C=US/ST=NY/CN=Nessus Certification Authority

192.168.0.54
Plugin Output

The following certificates were at the top of the certificate
chain sent by the remote host, but are signed by an unknown
certificate authority :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New
York/C=US/ST=NY/CN=Nessus Certification Authority
|-Issuer : O=Nessus Users United/OU=Nessus Certification Authority/L=New
York/C=US/ST=NY/CN=Nessus Certification Authority

192.168.0.53
Plugin Output

The following certificates were at the top of the certificate
chain sent by the remote host, but are signed by an unknown
certificate authority :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority
|-Issuer : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority

192.168.0.52
Plugin Output

The following certificates were at the top of the certificate
chain sent by the remote host, but are signed by an unknown
certificate authority :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority
|-Issuer : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority

192.168.0.41
Plugin Output

The following certificates were at the top of the certificate
chain sent by the remote host, but are signed by an unknown
certificate authority :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority
|-Issuer : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority

192.168.0.33
Plugin Output

The following certificates were at the top of the certificate
chain sent by the remote host, but are signed by an unknown
certificate authority :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority
|-Issuer : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority

192.168.0.25
Plugin Output

The following certificates were at the top of the certificate
chain sent by the remote host, but are signed by an unknown
certificate authority :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority
|-Issuer : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority

192.168.0.24
Plugin Output

The following certificates were at the top of the certificate
chain sent by the remote host, but are signed by an unknown
certificate authority :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority
|-Issuer : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority

192.168.0.23
Plugin Output

The following certificates were at the top of the certificate
chain sent by the remote host, but are signed by an unknown
certificate authority :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority
|-Issuer : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority

---

Description
The X.509 certificate of the remote host is not signed by a known
public certificate authority. If the remote host is a public host in
production, this nullifies the use of SSL as anyone could establish a
man in the middle attack against the remote host.

Solution
Purchase or generate a proper certificate for this service.

Risk Factor
Medium/ CVSS Base Score: 6.4
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin publication date: 2010/12/15

Plugin last modification date: 2012/01/17

Port nessus (1241/tcp)

Plugin ID: 51192
SSL Certificate signed with an unknown Certificate Authority

Synopsis

The SSL certificate for this service is signed by an unknown certificate authority.
List of Hosts

192.168.0.54
Plugin Output

The following certificates were at the top of the certificate
chain sent by the remote host, but are signed by an unknown
certificate authority :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority
|-Issuer : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority

192.168.0.53
Plugin Output

The following certificates were at the top of the certificate
chain sent by the remote host, but are signed by an unknown
certificate authority :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority
|-Issuer : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority

192.168.0.33
Plugin Output

The following certificates were at the top of the certificate
chain sent by the remote host, but are signed by an unknown
certificate authority :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New
York/C=US/ST=NY/CN=Nessus Certification Authority
|-Issuer : O=Nessus Users United/OU=Nessus Certification Authority/L=New
York/C=US/ST=NY/CN=Nessus Certification Authority

192.168.0.25
Plugin Output

The following certificates were at the top of the certificate
chain sent by the remote host, but are signed by an unknown
certificate authority :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New
York/C=US/ST=NY/CN=Nessus Certification Authority
|-Issuer : O=Nessus Users United/OU=Nessus Certification Authority/L=New
York/C=US/ST=NY/CN=Nessus Certification Authority

192.168.0.24
Plugin Output

The following certificates were at the top of the certificate
chain sent by the remote host, but are signed by an unknown
certificate authority :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New
York/C=US/ST=NY/CN=Nessus Certification Authority
|-Issuer : O=Nessus Users United/OU=Nessus Certification Authority/L=New
York/C=US/ST=NY/CN=Nessus Certification Authority

192.168.0.23
Plugin Output

The following certificates were at the top of the certificate
chain sent by the remote host, but are signed by an unknown
certificate authority :

|-Subject : O=Nessus Users United/OU=Nessus Certification Authority/L=New
York/C=US/ST=NY/CN=Nessus Certification Authority
|-Issuer : O=Nessus Users United/OU=Nessus Certification Authority/L=New
York/C=US/ST=NY/CN=Nessus Certification Authority

Description
The X.509 certificate of the remote host is not signed by a known public certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man in the middle attack against the remote host.

Solution
Purchase or generate a proper certificate for this service.

Risk Factor
Medium/ CVSS Base Score: 6.4
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

Plugin publication date: 2010/12/15

Plugin last modification date: 2012/01/17

Port ssh (22/tcp)

Plugin ID: 10881
SSH Protocol Versions Supported

Synopsis

A SSH server is running on the remote host.
List of Hosts

192.168.0.67
Plugin Output
The remote SSH daemon supports the following versions of the SSH protocol :

- 1.99
- 2.0

SSHv2 host key fingerprint : 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3

192.168.0.40
Plugin Output
The remote SSH daemon supports the following versions of the
SSH protocol :

- 1.99
- 2.0

SSHv2 host key fingerprint : d1:7d:e9:a8:58:83:f6:1c:82:b4:f1:98:2d:7f:58:30

192.168.0.21
Plugin Output
The remote SSH daemon supports the following versions of the
SSH protocol :

- 1.99
- 2.0

SSHv2 host key fingerprint : 10:cc:35:45:8e:f2:7a:a1:cc:db:a0:e8:bf:c7:73:3d

---

Description
This plugin determines the versions of the SSH protocol supported by
the remote SSH daemon.

Solution
n/a

Risk Factor
None

Plugin publication date: 2002/03/06

Plugin last modification date: 2011/03/30

Port (0/tcp)

Plugin ID: 56281
USN-1215-1 : apt vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : apt_0.7.25.3ubuntu9.4
Fixed package : apt_0.7.25.3ubuntu9.7

Description
It was discovered that the apt-key utility incorrectly verified GPG
keys when downloaded via the net-update option. If a remote attacker
were able to perform a man-in-the-middle attack, this flaw could
potentially be used to install altered packages. This update corrects
the issue by disabling the net-update option completely. A future
update will re-enable the option with corrected verification.

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1215-1/

Risk Factor
High

Other references
USN:1215-1

Patch publication date: 2011/09/22
Plugin publication date: 2011/09/23

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 56236
USN-1209-1 : ffmpeg vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : libavformat52_4:0.5.1-1ubuntu1.1
Fixed package : libavformat52_4:0.5.1-1ubuntu1.2

Description
It was discovered that FFmpeg incorrectly handled certain malformed ogg files. If a user were tricked into opening a crafted ogg file, an attacker could cause a denial of service via application crash, or possibly execute arbitrary code with the privileges of the user invoking the program. This issue only affected Ubuntu 10.10.

(CVE-2011-1196)

It was discovered that FFmpeg incorrectly handled certain malformed AMV files. If a user were tricked into opening a crafted AMV file, an attacker could cause a denial of service via application crash, or possibly execute arbitrary code with the privileges of the user invoking the program. This issue only affected Ubuntu 10.10. (CVE-2011-1931)

It was discovered that FFmpeg incorrectly handled certain malformed APE files. If a user were tricked into opening a crafted APE file, an attacker could cause a denial of service via application crash. (CVE-2011-2161)

Emmanouel Kellinis discovered that FFmpeg incorrectly handled certain malformed CAVS files. If a user were tricked into opening a crafted CAVS file, an attacker could cause a denial of service via application crash, or possibly execute arbitrary code with the privileges of the user invoking the program. (CVE-2011-3362)

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1209-1/

Risk Factor
High/ CVSS Base Score: 7.5
(CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVE
CVE-2011-1196
CVE-2011-1931
CVE-2011-2161
CVE-2011-3362

Other references
USN:1209-1

Patch publication date: 2011/09/19
Plugin publication date: 2011/09/20

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 57345
USN-1314-1 : python3.1, python3.2 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : python3.1-minimal_3.1.2-0ubuntu3
Fixed package : python3.1-minimal_3.1.2-0ubuntu3.1

Description
Giampaolo Rodola discovered that the smtpd module in Python 3 did not properly handle certain error conditions. A remote attacker could exploit this to cause a denial of service via daemon outage. This issue only affected Ubuntu 10.04 LTS. (CVE-2010-3493)

Niels Heinen discovered that the urllib module in Python 3 would process Location headers that specify a file:// URL. A remote attacker could use this to obtain sensitive information or cause a denial of service via resource consumption. (CVE-2011-1521)

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1314-1/

Risk Factor
Medium/ CVSS Base Score: 6.4
(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:P)

CVE
CVE-2010-3493
CVE-2011-1521

Other references
USN:1314-1

Patch publication date: 2011/12/19
Plugin publication date: 2011/12/20

Plugin last modification date: 2011/12/20

Port (0/tcp)

Plugin ID: 55699
USN-1175-1 : libpng vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

List of Hosts

192.168.0.25
Plugin Output

- Installed package : libpng12-0_1.2.42-1ubuntu2.1
Fixed package : libpng12-0_1.2.42-1ubuntu2.2

Description
Frank Busse discovered that libpng did not properly handle certain malformed PNG images. If a user or automated system were tricked into opening a crafted PNG file, an attacker could cause libpng to crash, resulting in a denial of service. This issue only affected Ubuntu 10.04 LTS, 10.10, and 11.04. (CVE-2011-2501)

It was discovered that libpng did not properly handle certain malformed PNG images. If a user or automated system were tricked into opening a crafted PNG file, an attacker could cause a denial of service or possibly execute arbitrary code with the privileges of the user invoking the program. (CVE-2011-2690)

Frank Busse discovered that libpng did not properly handle certain PNG images with invalid sCAL chunks. If a user or automated system were tricked into opening a crafted PNG file, an attacker could cause a denial of service or possibly execute arbitrary code with the privileges of the user invoking the program. (CVE-2011-2692)

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1175-1/

Risk Factor
Medium/ CVSS Base Score: 6.8
(CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVE
CVE-2011-2501
CVE-2011-2690
CVE-2011-2692

Other references
USN:1175-1

Patch publication date: 2011/07/26
Plugin publication date: 2011/07/27

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 55648
USN-1172-1 : logrotate vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : logrotate_3.7.8-4ubuntu2.1
Fixed package : logrotate_3.7.8-4ubuntu2.2

Description
It was discovered that logrotate incorrectly handled the creation of
new log files. Local users could possibly read log files if they were
opened before permissions were in place. This issue only affected

Ubuntu 8.04 LTS. (CVE-2011-1098)

It was discovered that logrotate incorrectly handled certain log file names when used with the shred option. Local attackers able to create log files with specially crafted filenames could use this issue to execute arbitrary code. This issue only affected Ubuntu 10.04 LTS, 10.10, and 11.04. (CVE-2011-1154)

It was discovered that logrotate incorrectly handled certain malformed log filenames. Local attackers able to create log files with specially crafted filenames could use this issue to cause logrotate to stop processing log files, resulting in a denial of service. (CVE-2011-1155)

It was discovered that logrotate incorrectly handled symlinks and hard links when processing log files. A local attacker having write access to a log file directory could use this issue to overwrite or read arbitrary files. This issue only affected Ubuntu 8.04 LTS. (CVE-2011-1548)

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1172-1/

Risk Factor

Medium/ CVSS Base Score: 6.9
(CVSS2#AV:L/AC:M/Au:N/C:C/I:C/A:C)

CVE

CVE-2011-1098
CVE-2011-1154
CVE-2011-1155
CVE-2011-1548

Other references
USN:1172-1

Patch publication date: 2011/07/21
Plugin publication date: 2011/07/22

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 57615
USN-1334-1 : libxml2 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : libxml2_2.7.6.dfsg-1ubuntu1.1
Fixed package : libxml2_2.7.6.dfsg-1ubuntu1.3

Description
It was discovered that libxml2 contained an off by one error. If a user or application linked against libxml2 were tricked into opening a specially crafted XML file, an attacker could cause the application to crash or possibly execute arbitrary code with the privileges of the user invoking the program. (CVE-2011-0216)

It was discovered that libxml2 is vulnerable to double-free conditions when parsing certain XML documents. This could allow a remote attacker to cause a denial of service. (CVE-2011-2821, CVE-2011-2834)

It was discovered that libxml2 did not properly detect end of file when parsing certain XML documents. An attacker could exploit this to crash applications linked against libxml2. (CVE-2011-3905)

It was discovered that libxml2 did not properly decode entity references with long names. If a user or application linked against libxml2 were tricked into opening a specially crafted XML file, an attacker could cause the application to crash or possibly execute arbitrary code with the privileges of the user invoking the program. (CVE-2011-3919)

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1334-1/

Risk Factor

High/ CVSS Base Score: 9.3
(CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVE

CVE-2011-0216
CVE-2011-2821
CVE-2011-2834
CVE-2011-3905
CVE-2011-3919

Other references

USN:1334-1

Patch publication date: 2012/01/19
Plugin publication date: 2012/01/20

Plugin last modification date: 2012/01/20

Port (0/tcp)

Plugin ID: 54615
Device Type

Synopsis

It is possible to guess the remote device type.
List of Hosts

192.168.0.67
Plugin Output
Remote device type : general-purpose
Confidence level : 95

192.168.0.59
Plugin Output
Remote device type : general-purpose
Confidence level : 65

192.168.0.54
Plugin Output
Remote device type : general-purpose
Confidence level : 65

192.168.0.53
Plugin Output
Remote device type : general-purpose
Confidence level : 65

192.168.0.52
Plugin Output
Remote device type : general-purpose
Confidence level : 65

192.168.0.41
Plugin Output
Remote device type : general-purpose
Confidence level : 65

192.168.0.40

Plugin Output
Remote device type : general-purpose
Confidence level : 95

192.168.0.33
Plugin Output
Remote device type : general-purpose
Confidence level : 65

192.168.0.25
Plugin Output
Remote device type : general-purpose
Confidence level : 100

192.168.0.24
Plugin Output
Remote device type : general-purpose
Confidence level : 65

192.168.0.23
Plugin Output
Remote device type : general-purpose
Confidence level : 65

192.168.0.21
Plugin Output
Remote device type : general-purpose
Confidence level : 70

Description
Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution
n/a

Risk Factor

None

Plugin publication date: 2011/05/23

Plugin last modification date: 2011/05/23

Port www (80/tcp)

Plugin ID: 43111
HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.
List of Hosts

192.168.0.67
Plugin Output
Based on the response to an OPTIONS request :

- HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

/
/icons

192.168.0.40
Plugin Output
Based on the response to an OPTIONS request :

- HTTP methods GET HEAD OPTIONS POST are allowed on :

/
/icons
/ubuntu
/xp

192.168.0.21
Plugin Output
Based on the response to an OPTIONS request :

- HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

/icons
/php

Description
By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Solution
n/a

Risk Factor
None

Plugin publication date: 2009/12/10

Plugin last modification date: 2011/07/08

Port (0/tcp)

Plugin ID: 55921
USN-1184-1 : firefox, xulrunner-1.9.2 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : xulrunner-1.9.2_1.9.2.17+build3+nobinonly-0ubuntu0.10.04.1
Fixed package : xulrunner-1.9.2_1.9.2.20+build1+nobinonly-0ubuntu0.10.04.1

Description
Gary Kwong, Igor Bukanov, and Bob Clary discovered multiple memory vulnerabilities in the browser rendering engine. An attacker could use these to possibly execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2011-2982)

It was discovered that a vulnerability in event management code could permit JavaScript to be run in the wrong context. This could potentially allow a malicious website to run code as another website or with escalated privileges within the browser. (CVE-2011-2981)

It was discovered that an SVG text manipulation routine contained a dangling pointer vulnerability. An attacker could potentially use this to crash Firefox or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2011-0084)

It was discovered that web content could receive chrome privileges if it registered for drop events and a browser tab element was dropped into the content area. This could potentially allow a malicious website to run code with escalated privileges within the browser. (CVE-2011-2984)

It was discovered that appendChild contained a dangling pointer vulnerability. An attacker could potentially use this to crash Firefox or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2011-2378)

It was discovered that data from other domains could be read when RegExp.input was set. This could potentially allow a malicious website access to private data from other domains. (CVE-2011-2983)

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1184-1/

Risk Factor
Critical/ CVSS Base Score: 10.0
(CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVE
CVE-2011-0084
CVE-2011-2378
CVE-2011-2981
CVE-2011-2982
CVE-2011-2983
CVE-2011-2984

Other references
USN:1184-1

Patch publication date: 2011/08/19
Plugin publication date: 2011/08/20

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 25202
Enumerate IPv6 Interfaces via SSH

Synopsis

This plugin enumerates IPv6 interfaces on a remote host.
List of Hosts

192.168.0.25
Plugin Output

The following IPv6 interfaces are set on the remote host :

- fe80::226a:8aff:fe00:36f2 (on interface eth0)
- ::1 (on interface lo)
- fe80::250:56ff:fec0:1 (on interface vmnet1)
- fe80::250:56ff:fec0:8 (on interface vmnet8)

Description
By connecting to the remote host via SSH with the supplied credentials, this plugin enumerates network interfaces configured with IPv6 addresses.

Solution
Disable IPv6 if you do not actually using it. Otherwise, disable any unused IPv6 interfaces.

Risk Factor
None

Plugin publication date: 2007/05/11

Plugin last modification date: 2011/03/21

Port ssh (22/tcp)

Plugin ID: 32314
Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

---

Synopsis

The remote SSH host keys are weak.

List of Hosts

192.168.0.67

192.168.0.21

Description
The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

Solution
Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

See also
http://www.nessus.org/u?5d01bdab
http://www.nessus.org/u?f14f4224

Risk Factor
Critical/ CVSS Base Score: 10.0
(CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)
CVSS Temporal Score: 8.3(CVSS2#E:F/RL:OF/RC:C)

CVE
CVE-2008-0166

Bugtraq ID
29179

Other references
OSVDB:45029
CWE:310

Plugin publication date: 2008/05/14
Plugin last modification date: 2011/03/21
Ease of exploitability: Exploits are available

Exploitable with: Core Impact

Port dns (53/udp)

Plugin ID: 35371
DNS Server hostname.bind Map Hostname Disclosure

Synopsis

The DNS server discloses the remote host name.
List of Hosts

192.168.0.67
Plugin Output

The remote host name is :

metasploitable

Description
It is possible to learn the remote host name by querying the remote
DNS server for 'hostname.bind' in the CHAOS domain.

Solution
It may be possible to disable this feature. Consult the vendor's documentation for more information.

Risk Factor
None

Plugin publication date: 2009/01/15

Plugin last modification date: 2011/09/14

Port www (80/tcp)

Plugin ID: 34850
Web Server Uses Basic Authentication Without HTTPS

Synopsis

The remote web server seems to transmit credentials in clear text.
List of Hosts

192.168.0.21
Plugin Output

The following pages are protected.
/php/phpMyAdmin/:/ realm="phpMyAdmin running on localhost"
/php/phpMyAdmin/?D=A:/ realm="phpMyAdmin running on localhost"

Description
The remote web server contains web pages that are protected by 'Basic' authentication over plain text.

An attacker eavesdropping the traffic might obtain logins and passwords

of valid users.

Solution
Make sure that HTTP authentication is transmitted over HTTPS.

Risk Factor
Low/ CVSS Base Score: 2.6
(CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

Plugin publication date: 2008/11/21

Plugin last modification date: 2011/09/15

Port www (8834/tcp)

Plugin ID: 10863
SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.
List of Hosts

192.168.0.59
Plugin Output
Subject Name:

Organization: Nessus Users United
Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY
Common Name: builder32-2

Issuer Name:

Organization: Nessus Users United
Organization Unit: Nessus Certification Authority
Locality: New York

Country: US
State/Province: NY
Common Name: Nessus Certification Authority

Serial Number: 00 B0 E7

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: May 10 16:11:59 2011 GMT
Not Valid After: May 09 16:11:59 2012 GMT

Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 97 04 CA 60 41 D5 FA BE 9F B5 60 DF 1B AF B6 44 58 C8 E7
21 C4 37 F0 FC 40 2F 69 5A 24 AF C0 E2 83 BA 50 55 2A 7E E2
A2 2E 0B CD E4 12 C2 46 6D 01 63 12 14 EF 62 86 B3 DA 4E 7B
39 26 8B CC 6D C5 C4 71 1F C2 5C 4F 68 2E B1 19 11 8E F0 4B
63 33 5C 8D 97 E4 9F 28 D5 27 F8 78 08 D2 04 C0 86 D1 0E 47
37 92 B1 D8 55 0D AB 33 EC C0 FA 00 68 DB 2C C1 BC 6E DB 95
F9 61 B7 DF F7 FE 7F 4A DF
Exponent: 01 00 01

Signature: 00 1A DF D1 E5 0B 80 67 06 7D 08 7C 7E 67 97 7E CD BB 2F F1
2D F0 19 96 24 0A 22 0A 4E 0D C4 15 A7 FD C2 50 7D E8 FC 80
61 1C D8 FC 8D 42 99 73 8F 1D 51 69 FC DE E2 9B 7C 21 79 76
56 1C 36 F2 C6 69 09 DA 91 A0 B5 2B 00 AF D7 FD 7F DD 21 A0
7F 3E 29 61 3F 23 D5 3D 59 59 E3 4C 05 B7 32 08 E1 8A 89 AD
86 39 09 45 6C CF BE 91 E8 EC 38 83 E5 0E 3F 5E DB BF 29 F0
E4 D5 66 6E D4 68 2E CA 83

Extension: 2.16.840.1.113730.1.1
Critical: 0
Data: 03 02 06 40

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature, Non Repudiation, Key Encipherment

192.168.0.54
Plugin Output
Subject Name:

Organization: Nessus Users United

Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY
Common Name: builder32-2

Issuer Name:

Organization: Nessus Users United
Organization Unit: Nessus Certification Authority
Locality: New York
Country: US
State/Province: NY
Common Name: Nessus Certification Authority

Serial Number: 00 B0 E7

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: May 10 16:11:59 2011 GMT
Not Valid After: May 09 16:11:59 2012 GMT

Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 97 04 CA 60 41 D5 FA BE 9F B5 60 DF 1B AF B6 44 58 C8 E7
21 C4 37 F0 FC 40 2F 69 5A 24 AF C0 E2 83 BA 50 55 2A 7E E2
A2 2E 0B CD E4 12 C2 46 6D 01 63 12 14 EF 62 86 B3 DA 4E 7B
39 26 8B CC 6D C5 C4 71 1F C2 5C 4F 68 2E B1 19 11 8E F0 4B
63 33 5C 8D 97 E4 9F 28 D5 27 F8 78 08 D2 04 C0 86 D1 0E 47
37 92 B1 D8 55 0D AB 33 EC C0 FA 00 68 DB 2C C1 BC 6E DB 95
F9 61 B7 DF F7 FE 7F 4A DF
Exponent: 01 00 01

Signature: 00 1A DF D1 E5 0B 80 67 06 7D 08 7C 7E 67 97 7E CD BB 2F F1
2D F0 19 96 24 0A 22 0A 4E 0D C4 15 A7 FD C2 50 7D E8 FC 80
61 1C D8 FC 8D 42 99 73 8F 1D 51 69 FC DE E2 9B 7C 21 79 76
56 1C 36 F2 C6 69 09 DA 91 A0 B5 2B 00 AF D7 FD 7F DD 21 A0
7F 3E 29 61 3F 23 D5 3D 59 59 E3 4C 05 B7 32 08 E1 8A 89 AD
86 39 09 45 6C CF BE 91 E8 EC 38 83 E5 0E 3F 5E DB BF 29 F0
E4 D5 66 6E D4 68 2E CA 83

Extension: 2.16.840.1.113730.1.1
Critical: 0
Data: 03 02 06 40

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature, Non Repudiation, Key Encipherment

192.168.0.53
Plugin Output
Subject Name:

Organization: Nessus Users United
Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY
Common Name: builder32-2

Issuer Name:

Organization: Nessus Users United
Organization Unit: Nessus Certification Authority
Locality: New York
Country: US
State/Province: NY
Common Name: Nessus Certification Authority

Serial Number: 00 B0 E7

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: May 10 16:11:59 2011 GMT
Not Valid After: May 09 16:11:59 2012 GMT

Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 97 04 CA 60 41 D5 FA BE 9F B5 60 DF 1B AF B6 44 58 C8 E7
21 C4 37 F0 FC 40 2F 69 5A 24 AF C0 E2 83 BA 50 55 2A 7E E2
A2 2E 0B CD E4 12 C2 46 6D 01 63 12 14 EF 62 86 B3 DA 4E 7B
39 26 8B CC 6D C5 C4 71 1F C2 5C 4F 68 2E B1 19 11 8E F0 4B
63 33 5C 8D 97 E4 9F 28 D5 27 F8 78 08 D2 04 C0 86 D1 0E 47
37 92 B1 D8 55 0D AB 33 EC C0 FA 00 68 DB 2C C1 BC 6E DB 95
F9 61 B7 DF F7 FE 7F 4A DF
Exponent: 01 00 01

Signature: 00 1A DF D1 E5 0B 80 67 06 7D 08 7C 7E 67 97 7E CD BB 2F F1

2D F0 19 96 24 0A 22 0A 4E 0D C4 15 A7 FD C2 50 7D E8 FC 80
61 1C D8 FC 8D 42 99 73 8F 1D 51 69 FC DE E2 9B 7C 21 79 76
56 1C 36 F2 C6 69 09 DA 91 A0 B5 2B 00 AF D7 FD 7F DD 21 A0
7F 3E 29 61 3F 23 D5 3D 59 59 E3 4C 05 B7 32 08 E1 8A 89 AD
86 39 09 45 6C CF BE 91 E8 EC 38 83 E5 0E 3F 5E DB BF 29 F0
E4 D5 66 6E D4 68 2E CA 83

Extension: 2.16.840.1.113730.1.1
Critical: 0
Data: 03 02 06 40

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature, Non Repudiation, Key Encipherment

192.168.0.52
Plugin Output
Subject Name:

Organization: Nessus Users United
Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY
Common Name: builder32-2

Issuer Name:

Organization: Nessus Users United
Organization Unit: Nessus Certification Authority
Locality: New York
Country: US
State/Province: NY
Common Name: Nessus Certification Authority

Serial Number: 00 B0 E7

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: May 10 16:11:59 2011 GMT
Not Valid After: May 09 16:11:59 2012 GMT

Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 97 04 CA 60 41 D5 FA BE 9F B5 60 DF 1B AF B6 44 58 C8 E7
21 C4 37 F0 FC 40 2F 69 5A 24 AF C0 E2 83 BA 50 55 2A 7E E2
A2 2E 0B CD E4 12 C2 46 6D 01 63 12 14 EF 62 86 B3 DA 4E 7B
39 26 8B CC 6D C5 C4 71 1F C2 5C 4F 68 2E B1 19 11 8E F0 4B
63 33 5C 8D 97 E4 9F 28 D5 27 F8 78 08 D2 04 C0 86 D1 0E 47
37 92 B1 D8 55 0D AB 33 EC C0 FA 00 68 DB 2C C1 BC 6E DB 95
F9 61 B7 DF F7 FE 7F 4A DF
Exponent: 01 00 01

Signature: 00 1A DF D1 E5 0B 80 67 06 7D 08 7C 7E 67 97 7E CD BB 2F F1
2D F0 19 96 24 0A 22 0A 4E 0D C4 15 A7 FD C2 50 7D E8 FC 80
61 1C D8 FC 8D 42 99 73 8F 1D 51 69 FC DE E2 9B 7C 21 79 76
56 1C 36 F2 C6 69 09 DA 91 A0 B5 2B 00 AF D7 FD 7F DD 21 A0
7F 3E 29 61 3F 23 D5 3D 59 59 E3 4C 05 B7 32 08 E1 8A 89 AD
86 39 09 45 6C CF BE 91 E8 EC 38 83 E5 0E 3F 5E DB BF 29 F0
E4 D5 66 6E D4 68 2E CA 83

Extension: 2.16.840.1.113730.1.1
Critical: 0
Data: 03 02 06 40

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature, Non Repudiation, Key Encipherment

192.168.0.41
Plugin Output
Subject Name:

Organization: Nessus Users United
Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY
Common Name: builder32-2

Issuer Name:

Organization: Nessus Users United
Organization Unit: Nessus Certification Authority
Locality: New York
Country: US
State/Province: NY
Common Name: Nessus Certification Authority

Serial Number: 00 B0 E7

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: May 10 16:11:59 2011 GMT
Not Valid After: May 09 16:11:59 2012 GMT

Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 97 04 CA 60 41 D5 FA BE 9F B5 60 DF 1B AF B6 44 58 C8 E7
21 C4 37 F0 FC 40 2F 69 5A 24 AF C0 E2 83 BA 50 55 2A 7E E2
A2 2E 0B CD E4 12 C2 46 6D 01 63 12 14 EF 62 86 B3 DA 4E 7B
39 26 8B CC 6D C5 C4 71 1F C2 5C 4F 68 2E B1 19 11 8E F0 4B
63 33 5C 8D 97 E4 9F 28 D5 27 F8 78 08 D2 04 C0 86 D1 0E 47
37 92 B1 D8 55 0D AB 33 EC C0 FA 00 68 DB 2C C1 BC 6E DB 95
F9 61 B7 DF F7 FE 7F 4A DF
Exponent: 01 00 01

Signature: 00 1A DF D1 E5 0B 80 67 06 7D 08 7C 7E 67 97 7E CD BB 2F F1
2D F0 19 96 24 0A 22 0A 4E 0D C4 15 A7 FD C2 50 7D E8 FC 80
61 1C D8 FC 8D 42 99 73 8F 1D 51 69 FC DE E2 9B 7C 21 79 76
56 1C 36 F2 C6 69 09 DA 91 A0 B5 2B 00 AF D7 FD 7F DD 21 A0
7F 3E 29 61 3F 23 D5 3D 59 59 E3 4C 05 B7 32 08 E1 8A 89 AD
86 39 09 45 6C CF BE 91 E8 EC 38 83 E5 0E 3F 5E DB BF 29 F0
E4 D5 66 6E D4 68 2E CA 83

Extension: 2.16.840.1.113730.1.1
Critical: 0
Data: 03 02 06 40

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature, Non Repudiation, Key Encipherment

192.168.0.33
Plugin Output
Subject Name:

Organization: Nessus Users United
Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY

Common Name: builder32-2

Issuer Name:

Organization: Nessus Users United
Organization Unit: Nessus Certification Authority
Locality: New York
Country: US
State/Province: NY
Common Name: Nessus Certification Authority

Serial Number: 00 B0 E7

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: May 10 16:11:59 2011 GMT
Not Valid After: May 09 16:11:59 2012 GMT

Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 97 04 CA 60 41 D5 FA BE 9F B5 60 DF 1B AF B6 44 58 C8 E7
21 C4 37 F0 FC 40 2F 69 5A 24 AF C0 E2 83 BA 50 55 2A 7E E2
A2 2E 0B CD E4 12 C2 46 6D 01 63 12 14 EF 62 86 B3 DA 4E 7B
39 26 8B CC 6D C5 C4 71 1F C2 5C 4F 68 2E B1 19 11 8E F0 4B
63 33 5C 8D 97 E4 9F 28 D5 27 F8 78 08 D2 04 C0 86 D1 0E 47
37 92 B1 D8 55 0D AB 33 EC C0 FA 00 68 DB 2C C1 BC 6E DB 95
F9 61 B7 DF F7 FE 7F 4A DF
Exponent: 01 00 01

Signature: 00 1A DF D1 E5 0B 80 67 06 7D 08 7C 7E 67 97 7E CD BB 2F F1
2D F0 19 96 24 0A 22 0A 4E 0D C4 15 A7 FD C2 50 7D E8 FC 80
61 1C D8 FC 8D 42 99 73 8F 1D 51 69 FC DE E2 9B 7C 21 79 76
56 1C 36 F2 C6 69 09 DA 91 A0 B5 2B 00 AF D7 FD 7F DD 21 A0
7F 3E 29 61 3F 23 D5 3D 59 59 E3 4C 05 B7 32 08 E1 8A 89 AD
86 39 09 45 6C CF BE 91 E8 EC 38 83 E5 0E 3F 5E DB BF 29 F0
E4 D5 66 6E D4 68 2E CA 83

Extension: 2.16.840.1.113730.1.1
Critical: 0
Data: 03 02 06 40

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature, Non Repudiation, Key Encipherment

192.168.0.25
Plugin Output
Subject Name:

Organization: Nessus Users United
Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY
Common Name: builder32-2

Issuer Name:

Organization: Nessus Users United
Organization Unit: Nessus Certification Authority
Locality: New York
Country: US
State/Province: NY
Common Name: Nessus Certification Authority

Serial Number: 00 B0 E7

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: May 10 16:11:59 2011 GMT
Not Valid After: May 09 16:11:59 2012 GMT

Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 97 04 CA 60 41 D5 FA BE 9F B5 60 DF 1B AF B6 44 58 C8 E7
21 C4 37 F0 FC 40 2F 69 5A 24 AF C0 E2 83 BA 50 55 2A 7E E2
A2 2E 0B CD E4 12 C2 46 6D 01 63 12 14 EF 62 86 B3 DA 4E 7B
39 26 8B CC 6D C5 C4 71 1F C2 5C 4F 68 2E B1 19 11 8E F0 4B
63 33 5C 8D 97 E4 9F 28 D5 27 F8 78 08 D2 04 C0 86 D1 0E 47
37 92 B1 D8 55 0D AB 33 EC C0 FA 00 68 DB 2C C1 BC 6E DB 95
F9 61 B7 DF F7 FE 7F 4A DF
Exponent: 01 00 01

Signature: 00 1A DF D1 E5 0B 80 67 06 7D 08 7C 7E 67 97 7E CD BB 2F F1
2D F0 19 96 24 0A 22 0A 4E 0D C4 15 A7 FD C2 50 7D E8 FC 80
61 1C D8 FC 8D 42 99 73 8F 1D 51 69 FC DE E2 9B 7C 21 79 76
56 1C 36 F2 C6 69 09 DA 91 A0 B5 2B 00 AF D7 FD 7F DD 21 A0
7F 3E 29 61 3F 23 D5 3D 59 59 E3 4C 05 B7 32 08 E1 8A 89 AD

86 39 09 45 6C CF BE 91 E8 EC 38 83 E5 0E 3F 5E DB BF 29 F0
E4 D5 66 6E D4 68 2E CA 83

Extension: 2.16.840.1.113730.1.1
Critical: 0
Data: 03 02 06 40

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature, Non Repudiation, Key Encipherment

192.168.0.24
Plugin Output
Subject Name:

Organization: Nessus Users United
Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY
Common Name: builder32-2

Issuer Name:

Organization: Nessus Users United
Organization Unit: Nessus Certification Authority
Locality: New York
Country: US
State/Province: NY
Common Name: Nessus Certification Authority

Serial Number: 00 B0 E7

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: May 10 16:11:59 2011 GMT
Not Valid After: May 09 16:11:59 2012 GMT

Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 97 04 CA 60 41 D5 FA BE 9F B5 60 DF 1B AF B6 44 58 C8 E7
21 C4 37 F0 FC 40 2F 69 5A 24 AF C0 E2 83 BA 50 55 2A 7E E2
A2 2E 0B CD E4 12 C2 46 6D 01 63 12 14 EF 62 86 B3 DA 4E 7B

39 26 8B CC 6D C5 C4 71 1F C2 5C 4F 68 2E B1 19 11 8E F0 4B
63 33 5C 8D 97 E4 9F 28 D5 27 F8 78 08 D2 04 C0 86 D1 0E 47
37 92 B1 D8 55 0D AB 33 EC C0 FA 00 68 DB 2C C1 BC 6E DB 95
F9 61 B7 DF F7 FE 7F 4A DF
Exponent: 01 00 01

Signature: 00 1A DF D1 E5 0B 80 67 06 7D 08 7C 7E 67 97 7E CD BB 2F F1
2D F0 19 96 24 0A 22 0A 4E 0D C4 15 A7 FD C2 50 7D E8 FC 80
61 1C D8 FC 8D 42 99 73 8F 1D 51 69 FC DE E2 9B 7C 21 79 76
56 1C 36 F2 C6 69 09 DA 91 A0 B5 2B 00 AF D7 FD 7F DD 21 A0
7F 3E 29 61 3F 23 D5 3D 59 59 E3 4C 05 B7 32 08 E1 8A 89 AD
86 39 09 45 6C CF BE 91 E8 EC 38 83 E5 0E 3F 5E DB BF 29 F0
E4 D5 66 6E D4 68 2E CA 83

Extension: 2.16.840.1.113730.1.1
Critical: 0
Data: 03 02 06 40

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature, Non Repudiation, Key Encipherment

192.168.0.23
Plugin Output
Subject Name:

Organization: Nessus Users United
Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY
Common Name: builder32-2

Issuer Name:

Organization: Nessus Users United
Organization Unit: Nessus Certification Authority
Locality: New York
Country: US
State/Province: NY
Common Name: Nessus Certification Authority

Serial Number: 00 B1 38

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: May 10 07:54:17 2011 GMT
Not Valid After: May 09 07:54:17 2012 GMT

Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 E2 6E 29 A6 0F CF BF 91 B5 19 55 C6 C1 E9 E8 00 DA 54 24
01 F5 36 E9 D2 B9 F9 41 05 87 E0 60 C6 34 04 D5 0C E1 B5 45
97 7D 07 C1 AA 1A F4 0B 12 E9 09 4E D9 33 D9 34 56 2B DF DB
01 1F C5 F3 D9 2B 18 4E 08 50 DB 68 56 F9 A5 1F 17 05 33 7F
2B 4D 92 69 F9 AF 57 A2 07 2A 95 49 15 55 02 5C A7 D0 0D 6E
F0 81 56 D8 C8 DA 15 31 F5 D4 A1 6B 5E 8E 5B 57 82 9C 1E 22
C6 CD 3D BF 99 7A 62 AB 4B
Exponent: 01 00 01

Signature: 00 94 D7 B0 DB 12 3D D2 CC B1 5D 7E 46 C5 6A 9F 1C BA C4 27
43 28 0A 0A 88 DA 6A 34 81 50 F5 E1 60 32 23 B6 5C 15 50 46
B1 11 C8 5B A5 6F 59 E5 02 F9 A6 C4 CB FA D3 F1 DB FC 8F 34
6F 7C 30 92 9E 20 DE 78 EE 38 BE E9 92 32 C5 DC 4A D4 E3 D6
C5 6D 38 CD 9D E8 7F 40 FF 6A BC B3 79 1A 64 61 04 7C 83 A2
D7 DD 35 2C C0 51 A6 EE B7 12 B0 A8 4D 9B 60 61 A7 33 EC F6
A3 B1 A4 4A DF 25 B4 76 AC

Extension: 2.16.840.1.113730.1.1
Critical: 0
Data: 03 02 06 40

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature, Non Repudiation, Key Encipherment

---

Description

This plugin connects to every SSL-related port and attempts to
extract and dump the X.509 certificate.

Solution

n/a

Risk Factor
None

Plugin publication date: 2008/05/19

Plugin last modification date: 2012/01/23

Port nessus (1241/tcp)

Plugin ID: 10863
SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.
List of Hosts

192.168.0.59
Plugin Output
Subject Name:

Organization: Nessus Users United
Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY
Common Name: builder32-2

Issuer Name:

Organization: Nessus Users United
Organization Unit: Nessus Certification Authority
Locality: New York
Country: US
State/Province: NY
Common Name: Nessus Certification Authority

Serial Number: 00 B0 E7

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: May 10 16:11:59 2011 GMT
Not Valid After: May 09 16:11:59 2012 GMT

Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 97 04 CA 60 41 D5 FA BE 9F B5 60 DF 1B AF B6 44 58 C8 E7
21 C4 37 F0 FC 40 2F 69 5A 24 AF C0 E2 83 BA 50 55 2A 7E E2
A2 2E 0B CD E4 12 C2 46 6D 01 63 12 14 EF 62 86 B3 DA 4E 7B
39 26 8B CC 6D C5 C4 71 1F C2 5C 4F 68 2E B1 19 11 8E F0 4B
63 33 5C 8D 97 E4 9F 28 D5 27 F8 78 08 D2 04 C0 86 D1 0E 47
37 92 B1 D8 55 0D AB 33 EC C0 FA 00 68 DB 2C C1 BC 6E DB 95
F9 61 B7 DF F7 FE 7F 4A DF
Exponent: 01 00 01

Signature: 00 1A DF D1 E5 0B 80 67 06 7D 08 7C 7E 67 97 7E CD BB 2F F1
2D F0 19 96 24 0A 22 0A 4E 0D C4 15 A7 FD C2 50 7D E8 FC 80
61 1C D8 FC 8D 42 99 73 8F 1D 51 69 FC DE E2 9B 7C 21 79 76
56 1C 36 F2 C6 69 09 DA 91 A0 B5 2B 00 AF D7 FD 7F DD 21 A0
7F 3E 29 61 3F 23 D5 3D 59 59 E3 4C 05 B7 32 08 E1 8A 89 AD
86 39 09 45 6C CF BE 91 E8 EC 38 83 E5 0E 3F 5E DB BF 29 F0
E4 D5 66 6E D4 68 2E CA 83

Extension: 2.16.840.1.113730.1.1
Critical: 0
Data: 03 02 06 40

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature, Non Repudiation, Key Encipherment

192.168.0.54
Plugin Output
Subject Name:

Organization: Nessus Users United
Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY
Common Name: builder32-2

Issuer Name:

Organization: Nessus Users United
Organization Unit: Nessus Certification Authority
Locality: New York
Country: US
State/Province: NY
Common Name: Nessus Certification Authority

Serial Number: 00 B0 E7

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: May 10 16:11:59 2011 GMT
Not Valid After: May 09 16:11:59 2012 GMT

Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 97 04 CA 60 41 D5 FA BE 9F B5 60 DF 1B AF B6 44 58 C8 E7
21 C4 37 F0 FC 40 2F 69 5A 24 AF C0 E2 83 BA 50 55 2A 7E E2
A2 2E 0B CD E4 12 C2 46 6D 01 63 12 14 EF 62 86 B3 DA 4E 7B
39 26 8B CC 6D C5 C4 71 1F C2 5C 4F 68 2E B1 19 11 8E F0 4B
63 33 5C 8D 97 E4 9F 28 D5 27 F8 78 08 D2 04 C0 86 D1 0E 47
37 92 B1 D8 55 0D AB 33 EC C0 FA 00 68 DB 2C C1 BC 6E DB 95
F9 61 B7 DF F7 FE 7F 4A DF
Exponent: 01 00 01

Signature: 00 1A DF D1 E5 0B 80 67 06 7D 08 7C 7E 67 97 7E CD BB 2F F1
2D F0 19 96 24 0A 22 0A 4E 0D C4 15 A7 FD C2 50 7D E8 FC 80
61 1C D8 FC 8D 42 99 73 8F 1D 51 69 FC DE E2 9B 7C 21 79 76
56 1C 36 F2 C6 69 09 DA 91 A0 B5 2B 00 AF D7 FD 7F DD 21 A0
7F 3E 29 61 3F 23 D5 3D 59 59 E3 4C 05 B7 32 08 E1 8A 89 AD
86 39 09 45 6C CF BE 91 E8 EC 38 83 E5 0E 3F 5E DB BF 29 F0
E4 D5 66 6E D4 68 2E CA 83

Extension: 2.16.840.1.113730.1.1
Critical: 0
Data: 03 02 06 40

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature, Non Repudiation, Key Encipherment

192.168.0.53

Plugin Output

Subject Name:

Organization: Nessus Users United
Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY
Common Name: builder32-2

Issuer Name:

Organization: Nessus Users United
Organization Unit: Nessus Certification Authority
Locality: New York
Country: US
State/Province: NY
Common Name: Nessus Certification Authority

Serial Number: 00 B0 E7

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: May 10 16:11:59 2011 GMT
Not Valid After: May 09 16:11:59 2012 GMT

Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 97 04 CA 60 41 D5 FA BE 9F B5 60 DF 1B AF B6 44 58 C8 E7
21 C4 37 F0 FC 40 2F 69 5A 24 AF C0 E2 83 BA 50 55 2A 7E E2
A2 2E 0B CD E4 12 C2 46 6D 01 63 12 14 EF 62 86 B3 DA 4E 7B
39 26 8B CC 6D C5 C4 71 1F C2 5C 4F 68 2E B1 19 11 8E F0 4B
63 33 5C 8D 97 E4 9F 28 D5 27 F8 78 08 D2 04 C0 86 D1 0E 47
37 92 B1 D8 55 0D AB 33 EC C0 FA 00 68 DB 2C C1 BC 6E DB 95
F9 61 B7 DF F7 FE 7F 4A DF
Exponent: 01 00 01

Signature: 00 1A DF D1 E5 0B 80 67 06 7D 08 7C 7E 67 97 7E CD BB 2F F1
2D F0 19 96 24 0A 22 0A 4E 0D C4 15 A7 FD C2 50 7D E8 FC 80
61 1C D8 FC 8D 42 99 73 8F 1D 51 69 FC DE E2 9B 7C 21 79 76
56 1C 36 F2 C6 69 09 DA 91 A0 B5 2B 00 AF D7 FD 7F DD 21 A0
7F 3E 29 61 3F 23 D5 3D 59 59 E3 4C 05 B7 32 08 E1 8A 89 AD
86 39 09 45 6C CF BE 91 E8 EC 38 83 E5 0E 3F 5E DB BF 29 F0
E4 D5 66 6E D4 68 2E CA 83

Extension: 2.16.840.1.113730.1.1
Critical: 0
Data: 03 02 06 40

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature, Non Repudiation, Key Encipherment

192.168.0.52
Plugin Output
Subject Name:

Organization: Nessus Users United
Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY
Common Name: builder32-2

Issuer Name:

Organization: Nessus Users United
Organization Unit: Nessus Certification Authority
Locality: New York
Country: US
State/Province: NY
Common Name: Nessus Certification Authority

Serial Number: 00 B0 E7

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: May 10 16:11:59 2011 GMT
Not Valid After: May 09 16:11:59 2012 GMT

Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 97 04 CA 60 41 D5 FA BE 9F B5 60 DF 1B AF B6 44 58 C8 E7
21 C4 37 F0 FC 40 2F 69 5A 24 AF C0 E2 83 BA 50 55 2A 7E E2
A2 2E 0B CD E4 12 C2 46 6D 01 63 12 14 EF 62 86 B3 DA 4E 7B
39 26 8B CC 6D C5 C4 71 1F C2 5C 4F 68 2E B1 19 11 8E F0 4B
63 33 5C 8D 97 E4 9F 28 D5 27 F8 78 08 D2 04 C0 86 D1 0E 47
37 92 B1 D8 55 0D AB 33 EC C0 FA 00 68 DB 2C C1 BC 6E DB 95

F9 61 B7 DF F7 FE 7F 4A DF
Exponent: 01 00 01

Signature: 00 1A DF D1 E5 0B 80 67 06 7D 08 7C 7E 67 97 7E CD BB 2F F1
2D F0 19 96 24 0A 22 0A 4E 0D C4 15 A7 FD C2 50 7D E8 FC 80
61 1C D8 FC 8D 42 99 73 8F 1D 51 69 FC DE E2 9B 7C 21 79 76
56 1C 36 F2 C6 69 09 DA 91 A0 B5 2B 00 AF D7 FD 7F DD 21 A0
7F 3E 29 61 3F 23 D5 3D 59 59 E3 4C 05 B7 32 08 E1 8A 89 AD
86 39 09 45 6C CF BE 91 E8 EC 38 83 E5 0E 3F 5E DB BF 29 F0
E4 D5 66 6E D4 68 2E CA 83

Extension: 2.16.840.1.113730.1.1
Critical: 0
Data: 03 02 06 40

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature, Non Repudiation, Key Encipherment

192.168.0.41
Plugin Output
Subject Name:

Organization: Nessus Users United
Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY
Common Name: builder32-2

Issuer Name:

Organization: Nessus Users United
Organization Unit: Nessus Certification Authority
Locality: New York
Country: US
State/Province: NY
Common Name: Nessus Certification Authority

Serial Number: 00 B0 E7

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: May 10 16:11:59 2011 GMT

Not Valid After: May 09 16:11:59 2012 GMT

Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 97 04 CA 60 41 D5 FA BE 9F B5 60 DF 1B AF B6 44 58 C8 E7
21 C4 37 F0 FC 40 2F 69 5A 24 AF C0 E2 83 BA 50 55 2A 7E E2
A2 2E 0B CD E4 12 C2 46 6D 01 63 12 14 EF 62 86 B3 DA 4E 7B
39 26 8B CC 6D C5 C4 71 1F C2 5C 4F 68 2E B1 19 11 8E F0 4B
63 33 5C 8D 97 E4 9F 28 D5 27 F8 78 08 D2 04 C0 86 D1 0E 47
37 92 B1 D8 55 0D AB 33 EC C0 FA 00 68 DB 2C C1 BC 6E DB 95
F9 61 B7 DF F7 FE 7F 4A DF
Exponent: 01 00 01

Signature: 00 1A DF D1 E5 0B 80 67 06 7D 08 7C 7E 67 97 7E CD BB 2F F1
2D F0 19 96 24 0A 22 0A 4E 0D C4 15 A7 FD C2 50 7D E8 FC 80
61 1C D8 FC 8D 42 99 73 8F 1D 51 69 FC DE E2 9B 7C 21 79 76
56 1C 36 F2 C6 69 09 DA 91 A0 B5 2B 00 AF D7 FD 7F DD 21 A0
7F 3E 29 61 3F 23 D5 3D 59 59 E3 4C 05 B7 32 08 E1 8A 89 AD
86 39 09 45 6C CF BE 91 E8 EC 38 83 E5 0E 3F 5E DB BF 29 F0
E4 D5 66 6E D4 68 2E CA 83

Extension: 2.16.840.1.113730.1.1
Critical: 0
Data: 03 02 06 40

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature, Non Repudiation, Key Encipherment

192.168.0.33
Plugin Output
Subject Name:

Organization: Nessus Users United
Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY
Common Name: builder32-2

Issuer Name:

Organization: Nessus Users United
Organization Unit: Nessus Certification Authority
Locality: New York

Country: US
State/Province: NY
Common Name: Nessus Certification Authority

Serial Number: 00 B0 E7

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: May 10 16:11:59 2011 GMT
Not Valid After: May 09 16:11:59 2012 GMT

Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 97 04 CA 60 41 D5 FA BE 9F B5 60 DF 1B AF B6 44 58 C8 E7
21 C4 37 F0 FC 40 2F 69 5A 24 AF C0 E2 83 BA 50 55 2A 7E E2
A2 2E 0B CD E4 12 C2 46 6D 01 63 12 14 EF 62 86 B3 DA 4E 7B
39 26 8B CC 6D C5 C4 71 1F C2 5C 4F 68 2E B1 19 11 8E F0 4B
63 33 5C 8D 97 E4 9F 28 D5 27 F8 78 08 D2 04 C0 86 D1 0E 47
37 92 B1 D8 55 0D AB 33 EC C0 FA 00 68 DB 2C C1 BC 6E DB 95
F9 61 B7 DF F7 FE 7F 4A DF
Exponent: 01 00 01

Signature: 00 1A DF D1 E5 0B 80 67 06 7D 08 7C 7E 67 97 7E CD BB 2F F1
2D F0 19 96 24 0A 22 0A 4E 0D C4 15 A7 FD C2 50 7D E8 FC 80
61 1C D8 FC 8D 42 99 73 8F 1D 51 69 FC DE E2 9B 7C 21 79 76
56 1C 36 F2 C6 69 09 DA 91 A0 B5 2B 00 AF D7 FD 7F DD 21 A0
7F 3E 29 61 3F 23 D5 3D 59 59 E3 4C 05 B7 32 08 E1 8A 89 AD
86 39 09 45 6C CF BE 91 E8 EC 38 83 E5 0E 3F 5E DB BF 29 F0
E4 D5 66 6E D4 68 2E CA 83

Extension: 2.16.840.1.113730.1.1
Critical: 0
Data: 03 02 06 40

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature, Non Repudiation, Key Encipherment

192.168.0.25
Plugin Output
Subject Name:

Organization: Nessus Users United

Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY
Common Name: builder32-2

Issuer Name:

Organization: Nessus Users United
Organization Unit: Nessus Certification Authority
Locality: New York
Country: US
State/Province: NY
Common Name: Nessus Certification Authority

Serial Number: 00 B0 E7

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: May 10 16:11:59 2011 GMT
Not Valid After: May 09 16:11:59 2012 GMT

Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 97 04 CA 60 41 D5 FA BE 9F B5 60 DF 1B AF B6 44 58 C8 E7
21 C4 37 F0 FC 40 2F 69 5A 24 AF C0 E2 83 BA 50 55 2A 7E E2
A2 2E 0B CD E4 12 C2 46 6D 01 63 12 14 EF 62 86 B3 DA 4E 7B
39 26 8B CC 6D C5 C4 71 1F C2 5C 4F 68 2E B1 19 11 8E F0 4B
63 33 5C 8D 97 E4 9F 28 D5 27 F8 78 08 D2 04 C0 86 D1 0E 47
37 92 B1 D8 55 0D AB 33 EC C0 FA 00 68 DB 2C C1 BC 6E DB 95
F9 61 B7 DF F7 FE 7F 4A DF
Exponent: 01 00 01

Signature: 00 1A DF D1 E5 0B 80 67 06 7D 08 7C 7E 67 97 7E CD BB 2F F1
2D F0 19 96 24 0A 22 0A 4E 0D C4 15 A7 FD C2 50 7D E8 FC 80
61 1C D8 FC 8D 42 99 73 8F 1D 51 69 FC DE E2 9B 7C 21 79 76
56 1C 36 F2 C6 69 09 DA 91 A0 B5 2B 00 AF D7 FD 7F DD 21 A0
7F 3E 29 61 3F 23 D5 3D 59 59 E3 4C 05 B7 32 08 E1 8A 89 AD
86 39 09 45 6C CF BE 91 E8 EC 38 83 E5 0E 3F 5E DB BF 29 F0
E4 D5 66 6E D4 68 2E CA 83

Extension: 2.16.840.1.113730.1.1
Critical: 0
Data: 03 02 06 40

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature, Non Repudiation, Key Encipherment

192.168.0.24
Plugin Output
Subject Name:

Organization: Nessus Users United
Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY
Common Name: builder32-2

Issuer Name:

Organization: Nessus Users United
Organization Unit: Nessus Certification Authority
Locality: New York
Country: US
State/Province: NY
Common Name: Nessus Certification Authority

Serial Number: 00 B0 E7

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: May 10 16:11:59 2011 GMT
Not Valid After: May 09 16:11:59 2012 GMT

Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 97 04 CA 60 41 D5 FA BE 9F B5 60 DF 1B AF B6 44 58 C8 E7
21 C4 37 F0 FC 40 2F 69 5A 24 AF C0 E2 83 BA 50 55 2A 7E E2
A2 2E 0B CD E4 12 C2 46 6D 01 63 12 14 EF 62 86 B3 DA 4E 7B
39 26 8B CC 6D C5 C4 71 1F C2 5C 4F 68 2E B1 19 11 8E F0 4B
63 33 5C 8D 97 E4 9F 28 D5 27 F8 78 08 D2 04 C0 86 D1 0E 47
37 92 B1 D8 55 0D AB 33 EC C0 FA 00 68 DB 2C C1 BC 6E DB 95
F9 61 B7 DF F7 FE 7F 4A DF
Exponent: 01 00 01

Signature: 00 1A DF D1 E5 0B 80 67 06 7D 08 7C 7E 67 97 7E CD BB 2F F1

2D F0 19 96 24 0A 22 0A 4E 0D C4 15 A7 FD C2 50 7D E8 FC 80
61 1C D8 FC 8D 42 99 73 8F 1D 51 69 FC DE E2 9B 7C 21 79 76
56 1C 36 F2 C6 69 09 DA 91 A0 B5 2B 00 AF D7 FD 7F DD 21 A0
7F 3E 29 61 3F 23 D5 3D 59 59 E3 4C 05 B7 32 08 E1 8A 89 AD
86 39 09 45 6C CF BE 91 E8 EC 38 83 E5 0E 3F 5E DB BF 29 F0
E4 D5 66 6E D4 68 2E CA 83

Extension: 2.16.840.1.113730.1.1
Critical: 0
Data: 03 02 06 40

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature, Non Repudiation, Key Encipherment

192.168.0.23
Plugin Output
Subject Name:

Organization: Nessus Users United
Organization Unit: Nessus Server
Locality: New York
Country: US
State/Province: NY
Common Name: builder32-2

Issuer Name:

Organization: Nessus Users United
Organization Unit: Nessus Certification Authority
Locality: New York
Country: US
State/Province: NY
Common Name: Nessus Certification Authority

Serial Number: 00 B1 38

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: May 10 07:54:17 2011 GMT
Not Valid After: May 09 07:54:17 2012 GMT

Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 E2 6E 29 A6 0F CF BF 91 B5 19 55 C6 C1 E9 E8 00 DA 54 24
01 F5 36 E9 D2 B9 F9 41 05 87 E0 60 C6 34 04 D5 0C E1 B5 45
97 7D 07 C1 AA 1A F4 0B 12 E9 09 4E D9 33 D9 34 56 2B DF DB
01 1F C5 F3 D9 2B 18 4E 08 50 DB 68 56 F9 A5 1F 17 05 33 7F
2B 4D 92 69 F9 AF 57 A2 07 2A 95 49 15 55 02 5C A7 D0 0D 6E
F0 81 56 D8 C8 DA 15 31 F5 D4 A1 6B 5E 8E 5B 57 82 9C 1E 22
C6 CD 3D BF 99 7A 62 AB 4B
Exponent: 01 00 01

Signature: 00 94 D7 B0 DB 12 3D D2 CC B1 5D 7E 46 C5 6A 9F 1C BA C4 27
43 28 0A 0A 88 DA 6A 34 81 50 F5 E1 60 32 23 B6 5C 15 50 46
B1 11 C8 5B A5 6F 59 E5 02 F9 A6 C4 CB FA D3 F1 DB FC 8F 34
6F 7C 30 92 9E 20 DE 78 EE 38 BE E9 92 32 C5 DC 4A D4 E3 D6
C5 6D 38 CD 9D E8 7F 40 FF 6A BC B3 79 1A 64 61 04 7C 83 A2
D7 DD 35 2C C0 51 A6 EE B7 12 B0 A8 4D 9B 60 61 A7 33 EC F6
A3 B1 A4 4A DF 25 B4 76 AC

Extension: 2.16.840.1.113730.1.1
Critical: 0
Data: 03 02 06 40

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature, Non Repudiation, Key Encipherment

---

Description

This plugin connects to every SSL-related port and attempts to
extract and dump the X.509 certificate.

Solution

n/a

Risk Factor

None

Plugin publication date: 2008/05/19

Plugin last modification date: 2012/01/23

Port (0/tcp)

Plugin ID: 55114
USN-1148-1 : libmodplug vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : libmodplug0c2_1:0.8.7-1build1
Fixed package : libmodplug0c2_1:0.8.7-1ubuntu0.2

Description
It was discovered that libmodplug did not correctly handle certain
malformed S3M media files. If a user or automated system were tricked
into opening a crafted S3M file, an attacker could cause a denial of
service or possibly execute arbitrary code with privileges of the
user invoking the program. (CVE-2011-1574)

It was discovered that libmodplug did not correctly handle certain
malformed ABC media files. If a user or automated system were tricked
into opening a crafted ABC file, an attacker could cause a denial of
service or possibly execute arbitrary code with privileges of the
user invoking the program. (CVE-2011-1761)

The default compiler options for affected releases should reduce the
vulnerability to a denial of service.

Solution

Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1148-1/

Risk Factor
Medium/ CVSS Base Score: 6.8
(CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P)

CVE
CVE-2011-1574
CVE-2011-1761

Other references
USN:1148-1

Patch publication date: 2011/06/13
Plugin publication date: 2011/06/14
Plugin last modification date: 2011/10/21
Ease of exploitability: Exploits are available

Exploitable with: Canvas (White_Phosphorus), Metasploit (VideoLAN VLC ModPlug ReadS3M Stack Buffer Overflow)

Port www (10000/tcp)

Plugin ID: 21785
Webmin / Usermin miniserv.pl Arbitrary File Disclosure

Synopsis

The remote web server is affected by an information disclosure flaw. access.
List of Hosts

192.168.0.21

Plugin Output

Here are the contents of the file '/etc/passwd' that Nessus was able to read from the remote host :

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
dhcp:x:100:101::/nonexistent:/bin/false
syslog:x:101:102::/home/syslog:/bin/false
klog:x:102:103::/home/klog:/bin/false
mysql:x:103:107:MySQL Server,,,:/var/lib/mysql:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
vmware:x:1000:1000:vmware,,,:/home/vmware:/bin/bash
obama:x:1001:1001::/home/obama:/bin/bash
osama:x:1002:1002::/home/osama:/bin/bash
yomama:x:1003:1003::/home/yomama:/bin/bash
```

Description

The remote host is running Webmin or Usermin, web-based interfaces for Unix / Linux system administrators and end-users.

Webmin and Usermin both come with the Perl script 'miniserv.pl' to provide basic web services, and the version of 'miniserv.pl' installed on the remote host contains a logic flaw that allows an unauthenticated attacker to read arbitrary files on the affected host, subject to the privileges of the web server user id.

Solution
Upgrade to Webmin 1.290 / Usermin 1.220 or later.

See also
http://www.webmin.com/changes-1.290.html
http://www.webmin.com/uchanges-1.220.html

Risk Factor
Medium/ CVSS Base Score: 5.0
(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)
CVSS Temporal Score: 4.1(CVSS2#E:F/RL:OF/RC:C)

CVE
CVE-2006-3392

Bugtraq ID
18744

Other references
OSVDB:26772

Vulnerability publication date: 2006/06/29
Plugin publication date: 2006/06/30
Plugin last modification date: 2011/03/14

Ease of exploitability: Exploits are available

Port (0/tcp)

Plugin ID: 45590
Common Platform Enumeration (CPE)

Synopsis

It is possible to enumerate CPE names that matched on the remote system.
List of Hosts

192.168.0.67
Plugin Output

The remote operating system matched the following CPE :

cpe:/o:canonical:ubuntu_linux:8.04

Following application CPE's matched on the remote system :

cpe:/a:openbsd:openssh:4.7
cpe:/a:samba:samba:3.0.20 -> Samba 3.0.20
cpe:/a:apache:http_server:2.2.8 -> Apache Software Foundation Apache HTTP Server 2.2.8
cpe:/a:php:php:5.2.4-2ubuntu5.10
cpe:/a:isc:bind:9.4.

192.168.0.59
Plugin Output

The remote operating system matched the following CPE :

cpe:/o:linux:linux_kernel:2.6

Following application CPE matched on the remote system :

cpe:/a:samba:samba:3.4.7 -> Samba 3.4.7

192.168.0.54
Plugin Output

The remote operating system matched the following CPE :

cpe:/o:linux:linux_kernel:2.6

Following application CPE matched on the remote system :

cpe:/a:samba:samba:3.4.7 -> Samba 3.4.7

192.168.0.53

Plugin Output

The remote operating system matched the following CPE :

cpe:/o:linux:linux_kernel:2.6

Following application CPE matched on the remote system :

cpe:/a:samba:samba:3.4.7 -> Samba 3.4.7

192.168.0.52
Plugin Output

The remote operating system matched the following CPE :

cpe:/o:linux:linux_kernel:2.6

Following application CPE matched on the remote system :

cpe:/a:samba:samba:3.4.7 -> Samba 3.4.7

192.168.0.41
Plugin Output

The remote operating system matched the following CPE :

cpe:/o:linux:linux_kernel:2.6

Following application CPE matched on the remote system :

cpe:/a:samba:samba:3.4.7 -> Samba 3.4.7

192.168.0.40
Plugin Output

The remote operating system matched the following CPE :

cpe:/o:canonical:ubuntu_linux:10.10

Following application CPE's matched on the remote system :

cpe:/a:openbsd:openssh:5.5
cpe:/a:apache:http_server:2.2.16 -> Apache Software Foundation Apache HTTP Server 2.2.16

192.168.0.33
Plugin Output

The remote operating system matched the following CPE :

cpe:/o:linux:linux_kernel:2.6

Following application CPE matched on the remote system :

cpe:/a:samba:samba:3.4.7 -> Samba 3.4.7

192.168.0.25
Plugin Output

The remote operating system matched the following CPE :

cpe:/o:canonical:ubuntu_linux:10.04

Following application CPE matched on the remote system :

cpe:/a:samba:samba:3.4.7 -> Samba 3.4.7

192.168.0.24
Plugin Output

The remote operating system matched the following CPE :

cpe:/o:linux:linux_kernel:2.6

Following application CPE matched on the remote system :

cpe:/a:samba:samba:3.4.7 -> Samba 3.4.7

192.168.0.23
Plugin Output

The remote operating system matched the following CPE :

cpe:/o:linux:linux_kernel:2.6

192.168.0.21
Plugin Output

The remote operating system matched the following CPE :

cpe:/o:linux:linux_kernel:2.6

Following application CPE's matched on the remote system :

cpe:/a:openbsd:openssh:4.6 -> OpenBSD OpenSSH 4.6
cpe:/a:samba:samba:3.0.26 -> Samba 3.0.26

cpe:/a:apache:http_server:2.2.4 -> Apache Software Foundation Apache HTTP Server 2.2.4
cpe:/a:php:php:5.2.3-1ubuntu6

Description
By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

Solution
n/a

See also
http://cpe.mitre.org/

Risk Factor
None

Plugin publication date: 2010/04/21

Plugin last modification date: 2012/01/19

Port ssh (22/tcp)

Plugin ID: 39520
Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.
List of Hosts

192.168.0.67
Plugin Output
Give Nessus credentials to perform local checks.

192.168.0.40
Plugin Output
Give Nessus credentials to perform local checks.

192.168.0.21
Plugin Output
Give Nessus credentials to perform local checks.

Description
Security patches may have been 'back ported' to the remote SSH server
without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any
security problem.

Solution
N/A

See also
http://www.nessus.org/u?d636c8c7

Risk Factor
None

Plugin publication date: 2009/06/25

Plugin last modification date: 2011/03/16

Port www (80/tcp)

Plugin ID: 39521
Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.
List of Hosts

192.168.0.67
Plugin Output
Give Nessus credentials to perform local checks.

192.168.0.40
Plugin Output
Give Nessus credentials to perform local checks.

192.168.0.21
Plugin Output
Give Nessus credentials to perform local checks.

Description
Security patches may have been 'back ported' to the remote HTTP server
without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any
security problem.

Solution
N/A

See also
http://www.nessus.org/u?d636c8c7

Risk Factor
None

Plugin publication date: 2009/06/25

Plugin last modification date: 2011/03/18

Port (0/tcp)

Plugin ID: 56140
USN-1197-5 : ca-certificates vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : ca-certificates_20090814
Fixed package : ca-certificates_20090814ubuntu0.10.04.1

Description
USN-1197-1 addressed an issue in Firefox and Xulrunner pertaining to the Dutch Certificate Authority DigiNotar mis-issuing fraudulent certificates. This update provides the corresponding update for ca-certificates.

Original advisory details:

It was discovered that Dutch Certificate Authority DigiNotar, had mis-issued multiple fraudulent certificates. These certificates could allow an attacker to perform a 'man in the middle' (MITM) attack which would make the user believe their connection is secure, but is actually being monitored.

For the protection of its users, Mozilla has removed the DigiNotar certificate. Sites using certificates issued by DigiNotar will need to seek another certificate vendor.

We are currently aware of a regression that blocks one of two Staat der Nederlanden root certificates which are believed to still be secure. This regression is being tracked at https://launchpad.net/bugs/838322.

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1197-5/

Risk Factor
High

Other references
USN:1197-5

Patch publication date: 2011/09/09
Plugin publication date: 2011/09/09

Plugin last modification date: 2011/10/21

Port (0/udp)

Plugin ID: 10287
Traceroute Information

Synopsis

It was possible to obtain traceroute information.
List of Hosts

192.168.0.67
Plugin Output
For your information, here is the traceroute from 192.168.0.25 to 192.168.0.67 :
192.168.0.25
192.168.0.67

192.168.0.59
Plugin Output
For your information, here is the traceroute from 192.168.0.25 to 192.168.0.59 :
192.168.0.25
192.168.0.59

192.168.0.54
Plugin Output
For your information, here is the traceroute from 192.168.0.25 to 192.168.0.54 :
192.168.0.25
192.168.0.54

192.168.0.53
Plugin Output
For your information, here is the traceroute from 192.168.0.25 to 192.168.0.53 :
192.168.0.25
192.168.0.53

192.168.0.52
Plugin Output
For your information, here is the traceroute from 192.168.0.25 to 192.168.0.52 :
192.168.0.25
192.168.0.52

192.168.0.41
Plugin Output
For your information, here is the traceroute from 192.168.0.25 to 192.168.0.41 :
192.168.0.25
192.168.0.41

192.168.0.40
Plugin Output

For your information, here is the traceroute from 192.168.0.25 to 192.168.0.40 :
192.168.0.25
192.168.0.40

192.168.0.33
Plugin Output
For your information, here is the traceroute from 192.168.0.25 to 192.168.0.33 :
192.168.0.25
192.168.0.33

192.168.0.24
Plugin Output
For your information, here is the traceroute from 192.168.0.25 to 192.168.0.24 :
192.168.0.25
192.168.0.24

192.168.0.23
Plugin Output
For your information, here is the traceroute from 192.168.0.25 to 192.168.0.23 :
192.168.0.25
192.168.0.23

192.168.0.21
Plugin Output
For your information, here is the traceroute from 192.168.0.25 to 192.168.0.21 :
192.168.0.25
192.168.0.21

Description
Makes a traceroute to the remote host.

Solution
n/a

Risk Factor
None

Plugin publication date: 1999/11/27

Plugin last modification date: 2011/03/21

Port (0/tcp)

Plugin ID: 12634
Authenticated Check: OS Name and Installed Package Enumeration

---

Synopsis

This plugin gathers information about the remote host via an authenticated session.

List of Hosts

192.168.0.25

Plugin Output

Nessus can run commands on localhost to check if patches are applied
The output of "uname -a" is :
Linux bt 2.6.39.4 #1 SMP Thu Aug 18 13:38:02 NZST 2011 i686 GNU/Linux

The remote Debian system is :
squeeze/sid

This is a Ubuntu system

Local security checks have been enabled for this host.

Description

This plugin logs into the remote host using SSH, RSH, RLOGIN, Telnet
or local commands and extracts the list of installed packages.

If using SSH, the scan should be configured with a valid SSH public
key and possibly an SSH passphrase (if the SSH public key is protected
by a passphrase).

Solution

n/a

Risk Factor
None

Plugin publication date: 2004/07/06

Plugin last modification date: 2011/12/23

Port (0/tcp)

Plugin ID: 55967
USN-1195-1 : webkit vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : libwebkit-1.0-2_1.2.5-0ubuntu0.10.04.1
Fixed package : libwebkit-1.0-2_1.2.7-0ubuntu0.10.04.1

Description
A large number of security issues were discovered in the WebKit browser and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1195-1/

Risk Factor
Critical/ CVSS Base Score: 10.0
(CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVE
CVE-2010-1824
CVE-2010-2646
CVE-2010-2651
CVE-2010-2900
CVE-2010-2901
CVE-2010-3120
CVE-2010-3254
CVE-2010-3812
CVE-2010-3813
CVE-2010-4040
CVE-2010-4042
CVE-2010-4197
CVE-2010-4198
CVE-2010-4199
CVE-2010-4204
CVE-2010-4206
CVE-2010-4492
CVE-2010-4493
CVE-2010-4577
CVE-2010-4578
CVE-2011-0482
CVE-2011-0778

Other references
USN:1195-1

Patch publication date: 2011/08/23
Plugin publication date: 2011/08/24

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 56330
USN-1210-1 : firefox, xulrunner-1.9.2 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : xulrunner-1.9.2_1.9.2.17+build3+nobinonly-0ubuntu0.10.04.1
Fixed package : xulrunner-1.9.2_1.9.2.23+build1+nobinonly-0ubuntu0.10.04.1

Description
Benjamin Smedberg, Bob Clary, Jesse Ruderman, and Josh Aas discovered multiple memory vulnerabilities in the browser rendering engine. An attacker could use these to possibly execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2011-2995, CVE-2011-2996)

Boris Zbarsky discovered that a frame named 'location' could shadow the window.location object unless a script in a page grabbed a reference to the true object before the frame was created. This is in violation of the Same Origin Policy. A malicious website could possibly use this to access another website or the local file system. (CVE-2011-2999)

Mark Kaplan discovered an integer underflow in the SpiderMonkey JavaScript engine. An attacker could potentially use this to crash Firefox.

Ian Graham discovered that when multiple Location headers were present, Firefox would use the second one resulting in a possible

CRLF injection attack. CRLF injection issues can result in a wide variety of attacks, such as XSS (Cross-Site Scripting) vulnerabilities, browser cache poisoning, and cookie theft. (CVE-2011-3000)

Mariusz Mlynski discovered that if the user could be convinced to hold down the enter key, a malicious website could potential pop up a download dialog and the default open action would be selected. This would result in potentially malicious content being run with privileges of the user invoking Firefox. (CVE-2011-2372)

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1210-1/

Risk Factor

Critical/ CVSS Base Score: 10.0
(CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVE

CVE-2011-2372
CVE-2011-2995
CVE-2011-2996
CVE-2011-2999
CVE-2011-3000
CVE-2011-3001

Other references

IAVA:2011-A-0133
USN:1210-1

Patch publication date: 2011/09/28
Plugin publication date: 2011/09/29

Plugin last modification date: 2011/12/12

Port (0/tcp)

Plugin ID: 55108
USN-1145-1 : qemu-kvm vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

List of Hosts

192.168.0.25

Plugin Output

- Installed package : qemu-kvm_0.12.3+noroms-0ubuntu9.6
Fixed package : qemu-kvm_0.12.3+noroms-0ubuntu9.9

Description

It was discovered that QEMU did not properly perform validation of I/O operations from the guest which could lead to heap corruption. An attacker could exploit this to cause a denial of service of the guest or possibly execute code with the privileges of the user invoking the program. (CVE-2011-1750)

Nelson Elhage discoverd that QEMU did not properly handle memory when removing ISA devices. An attacker could exploit this to cause a denial of service of the guest or possibly execute code with the privileges of the user invoking the program. (CVE-2011-1751)

When using QEMU with libvirt or virtualization management software based on libvirt such as Eucalyptus and OpenStack, QEMU guests are individually isolated by an AppArmor profile by default in Ubuntu.

Solution

Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1145-1/

Risk Factor
High

CVE
CVE-2011-1750
CVE-2011-1751

Other references
USN:1145-1

Patch publication date: 2011/06/09
Plugin publication date: 2011/06/13

Plugin last modification date: 2011/10/21

Port mdns (5353/udp)

Plugin ID: 12218
mDNS Detection

Synopsis

It is possible to obtain information about the remote host.
List of Hosts

192.168.0.40
Plugin Output
Nessus was able to extract the following information :

- mDNS hostname : is2c-dojo.local.

- Advertised services :
o Service name : is2c-dojo [10:78:d2:36:65:a4]._workstation._tcp.local.
Port number : 9
o Service name : saned._sane-port._tcp.local.
Port number : 6566

- CPU type : I686
- OS : LINUX

Description
The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running.

Solution
Filter incoming traffic to UDP port 5353 if desired.

Risk Factor
Medium/ CVSS Base Score: 5.0
(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin publication date: 2004/04/28

Plugin last modification date: 2011/03/11

Port www (10000/tcp)

Plugin ID: 10757
Webmin Detection

Synopsis

An administration service is running on the remote host.

List of Hosts

192.168.0.21

Description

The remote server is running Webmin, a web-based interface for system administration for Unix.

Solution

Stop the Webmin service if not needed or ensure access is limited to authorized hosts. See the menu items '[Webmin Configuration][IP Access Control]' and/or '[Webmin Configuration][Port and Address]'.

See also

http://www.webmin.net/

Risk Factor

None

Plugin publication date: 2001/09/14

Plugin last modification date: 2011/03/17

Port nessus (1241/tcp)

Plugin ID: 50845

OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

List of Hosts

192.168.0.59

192.168.0.54

192.168.0.53

192.168.0.52

192.168.0.41

192.168.0.33

192.168.0.25

192.168.0.24

192.168.0.23

Description
Based on its behavior, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

Solution
n/a

See also
http://www.openssl.org

Risk Factor
None

Plugin publication date: 2010/11/30

Plugin last modification date: 2011/04/20

Port dns (53/udp)

Plugin ID: 10028
DNS Server BIND version Directive Remote Version Disclosure

Synopsis

It is possible to obtain the version number of the remote DNS server.

List of Hosts

192.168.0.67

Plugin Output

The version of the remote DNS server is :

9.4.2

Description

The remote host is running BIND or another DNS server that reports its version number when it receives a special request, for the text 'version.bind' in the domain 'chaos'.

This version is not necessarily accurate and could even be forged, as some DNS servers send the information based on a configuration file.

Solution

It is possible to hide the version number of bind by using the 'version' directive in the 'options' section in named.conf

---

Risk Factor

None

Other references
OSVDB:23

Vulnerability publication date: 1991/01/01
Plugin publication date: 1999/10/12

Plugin last modification date: 2011/05/24

Port (0/tcp)

Plugin ID: 55407
USN-1149-1 : firefox, xulrunner-1.9.2 vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : xulrunner-1.9.2_1.9.2.17+build3+nobinonly-0ubuntu0.10.04.1
Fixed package : xulrunner-1.9.2_1.9.2.18+build2+nobinonly-0ubuntu0.10.04.1

Description
Multiple memory vulnerabilities were discovered in the browser
rendering engine. An attacker could use these to possibly execute
arbitrary code with the privileges of the user invoking Firefox.
(CVE-2011-2364, CVE-2011-2365, CVE-2011-2374, CVE-2011-2376)

Martin Barbella discovered that under certain conditions, viewing a
XUL document while JavaScript was disabled caused deleted memory to
be accessed. An attacker could potentially use this to crash Firefox
or execute arbitrary code with the privileges of the user invoking
Firefox. (CVE-2011-2373)

Jordi Chancel discovered a vulnerability on multipart/x-mixed-replace images due to memory corruption. An attacker could potentially use this to crash Firefox or execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2011-2377)

Chris Rohlf and Yan Ivnitskiy discovered an integer overflow vulnerability in JavaScript Arrays. An attacker could potentially use this to execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2011-2371)

Multiple use-after-free vulnerabilities were discovered. An attacker could potentially use these to execute arbitrary code with the privileges of the user invoking Firefox. (CVE-2011-0083, CVE-2011-0085, CVE-2011-2363)

David Chan discovered that cookies did not honor same-origin conventions. This could potentially lead to cookie data being leaked to a third party. (CVE-2011-2362)

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1149-1/

Risk Factor
Critical/ CVSS Base Score: 10.0
(CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVE
CVE-2011-0083
CVE-2011-0085
CVE-2011-2362
CVE-2011-2363
CVE-2011-2364
CVE-2011-2365
CVE-2011-2371
CVE-2011-2373

CVE-2011-2374
CVE-2011-2376
CVE-2011-2377

Other references
USN:1149-1

Patch publication date: 2011/06/22
Plugin publication date: 2011/06/23
Plugin last modification date: 2011/10/21
Ease of exploitability: Exploits are available

Exploitable with: Metasploit (windows/browser/mozilla_reduceright.rb)

Port cifs (445/tcp)

Plugin ID: 10394
Microsoft Windows SMB Log In Possible

Synopsis

It is possible to log into the remote host.
List of Hosts

192.168.0.67
Plugin Output
- NULL sessions are enabled on the remote host

192.168.0.59
Plugin Output
- NULL sessions are enabled on the remote host
- Remote users are authenticated as 'Guest'

192.168.0.54
Plugin Output
- NULL sessions are enabled on the remote host
- Remote users are authenticated as 'Guest'

192.168.0.53
Plugin Output
- NULL sessions are enabled on the remote host

- Remote users are authenticated as 'Guest'

192.168.0.52
Plugin Output
- NULL sessions are enabled on the remote host
- Remote users are authenticated as 'Guest'

192.168.0.41
Plugin Output
- NULL sessions are enabled on the remote host
- Remote users are authenticated as 'Guest'

192.168.0.33
Plugin Output
- NULL sessions are enabled on the remote host
- Remote users are authenticated as 'Guest'

192.168.0.25
Plugin Output
- NULL sessions are enabled on the remote host
- Remote users are authenticated as 'Guest'

192.168.0.24
Plugin Output
- NULL sessions are enabled on the remote host
- Remote users are authenticated as 'Guest'

192.168.0.21
Plugin Output
- NULL sessions are enabled on the remote host

Description
The remote host is running Microsoft Windows operating system or Samba, a CIFS/SMB server for Unix. It was possible to log into it using one of the following accounts :

- NULL session
- Guest account
- Given Credentials

Solution
n/a

See also
http://support.microsoft.com/support/kb/articles/Q143/4/74.ASP
http://support.microsoft.com/support/kb/articles/Q246/2/61.ASP

Risk Factor
None

Vulnerability publication date: 1999/01/01
Plugin publication date: 2000/05/09
Plugin last modification date: 2011/09/15
Ease of exploitability: Exploits are available

Exploitable with: Metasploit (Microsoft Windows Authenticated User Code Execution)

Port (0/tcp)

Plugin ID: 55982
USN-1185-1 : thunderbird vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : thunderbird_3.1.10+build1+nobinonly-0ubuntu0.10.04.1
Fixed package : thunderbird_3.1.12+build1+nobinonly-0ubuntu0.10.04.1

Description

Gary Kwong, Igor Bukanov, and Bob Clary discovered multiple memory vulnerabilities in the Gecko rendering engine. An attacker could use these to possibly execute arbitrary code with the privileges of the user invoking Thunderbird. (CVE-2011-2982)

It was discovered that a vulnerability in event management code could permit JavaScript to be run in the wrong context. This could potentially allow a malicious website to run code as another website or with escalated privileges in a chrome-privileged context. (CVE-2011-2981)

It was discovered that an SVG text manipulation routine contained a dangling pointer vulnerability. An attacker could potentially use this to crash Thunderbird or execute arbitrary code with the privileges of the user invoking Thunderbird. (CVE-2011-0084)

It was discovered that web content could receive chrome privileges if it registered for drop events and a browser tab element was dropped into the content area. This could potentially allow a malicious website to run code with escalated privileges within Thunderbird. (CVE-2011-2984)

It was discovered that appendChild contained a dangling pointer vulnerability. An attacker could potentially use this to crash Thunderbird or execute arbitrary code with the privileges of the user invoking Thunderbird. (CVE-2011-2378)

It was discovered that data from other domains could be read when RegExp.input was set. This could potentially allow a malicious website access to private data from other domains. (CVE-2011-2983)

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1185-1/

Risk Factor

Critical/ CVSS Base Score: 10.0
(CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVE
CVE-2011-0084
CVE-2011-2378
CVE-2011-2981
CVE-2011-2982
CVE-2011-2983
CVE-2011-2984

Other references
USN:1185-1

Patch publication date: 2011/08/26
Plugin publication date: 2011/08/26

Plugin last modification date: 2011/10/21

Port (0/tcp)

Plugin ID: 56389
USN-1226-1 : samba vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : smbfs_2:3.4.7~dfsg-1ubuntu3.6
Fixed package : smbfs_2:3.4.7~dfsg-1ubuntu3.8

Description

Dan Rosenberg discovered that Samba incorrectly handled changes to the mtab file. A local attacker could use this issue to corrupt the mtab file, possibly leading to a denial of service. (CVE-2011-1678)

Jan Lieskovsky discovered that Samba incorrectly filtered certain strings being added to the mtab file. A local attacker could use this issue to corrupt the mtab file, possibly leading to a denial of service. This issue only affected Ubuntu 10.04 LTS. (CVE-2011-2724)

Dan Rosenberg discovered that Samba incorrectly handled the mtab lock file. A local attacker could use this issue to create a stale lock file, possibly leading to a denial of service. (CVE-2011-3585)

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1226-1/

Risk Factor

Low/ CVSS Base Score: 3.3
(CVSS2#AV:L/AC:M/Au:N/C:P/I:P/A:N)

CVE

CVE-2011-1678
CVE-2011-2724
CVE-2011-3585

Other references

USN:1226-1

Patch publication date: 2011/10/04
Plugin publication date: 2011/10/05

Plugin last modification date: 2011/10/21

Port postgresql (5432/tcp)

Plugin ID: 26024
PostgreSQL Server Detection

Synopsis

A database service is listening on the remote host.
List of Hosts

192.168.0.67

Description
The remote service is a PostgreSQL database server, or a derivative
such as EnterpriseDB.

Solution
Limit incoming traffic to this port if desired.

See also
http://www.postgresql.org/

Risk Factor
None

Plugin publication date: 2007/09/14

Plugin last modification date: 2011/03/11

Port cifs (445/tcp)

Plugin ID: 10397
Microsoft Windows SMB LanMan Pipe Server Listing Disclosure

Synopsis

It is possible to obtain network information.
List of Hosts

192.168.0.67
Plugin Output

Here is the browse list of the remote host :

BT (os : 0.0)
METASPLOITABLE (os : 0.0)
VICTIM-EFA334F3 (os : 0.0)

192.168.0.59
Plugin Output

Here is the browse list of the remote host :

BT (os : 0.0)
METASPLOITABLE (os : 0.0)

192.168.0.54
Plugin Output

Here is the browse list of the remote host :

BT (os : 0.0)
METASPLOITABLE (os : 0.0)

192.168.0.53
Plugin Output

Here is the browse list of the remote host :

BT (os : 0.0)
METASPLOITABLE (os : 0.0)

192.168.0.52
Plugin Output

Here is the browse list of the remote host :

BT (os : 0.0)
METASPLOITABLE (os : 0.0)

192.168.0.41
Plugin Output

Here is the browse list of the remote host :

BT (os : 0.0)
METASPLOITABLE (os : 0.0)

192.168.0.33
Plugin Output

Here is the browse list of the remote host :

BT (os : 0.0)
METASPLOITABLE (os : 0.0)

192.168.0.25
Plugin Output

Here is the browse list of the remote host :

BT (os : 0.0)

192.168.0.24
Plugin Output

Here is the browse list of the remote host :

BT (os : 0.0)
METASPLOITABLE (os : 0.0)

192.168.0.21
Plugin Output

Here is the browse list of the remote host :

UBUNTUVM (os : 0.0)

Description
It was possible to obtain the browse list of the remote Windows system by sending a request to the LANMAN pipe. The browse list is the list of the nearest Windows systems of the remote host.

Solution
n/a

Risk Factor
None

Other references
OSVDB:300

Vulnerability publication date: 2000/01/01
Plugin publication date: 2000/05/09

Plugin last modification date: 2011/09/14

Port (0/tcp)

Plugin ID: 55099
USN-1138-1 : dbus-glib vulnerability

Synopsis

The remote Ubuntu host is missing one or more security-related patches.
List of Hosts

192.168.0.25
Plugin Output

- Installed package : libdbus-glib-1-2_0.84-1

Fixed package : libdbus-glib-1-2_0.84-1ubuntu0.2

Description
It was discovered that DBus-GLib did not properly verify the access flag of exported GObject properties under certain circumstances. A local attacker could exploit this to bypass intended access restrictions or possibly cause a denial of service.

Solution
Update the affected package(s).

See also
http://www.ubuntu.com/usn/usn-1138-1/

Risk Factor
Low/ CVSS Base Score: 2.1
(CVSS2#AV:L/AC:L/Au:N/C:N/I:N/A:P)

CVE
CVE-2010-1172

Other references
USN:1138-1

Patch publication date: 2011/05/26
Plugin publication date: 2011/06/13

Plugin last modification date: 2011/10/21

Port www (80/tcp)

Plugin ID: 46803
PHP expose_php Information Disclosure

Synopsis

The configuration of PHP on the remote host allows disclosure of sensitive information.
List of Hosts

192.168.0.21
Plugin Output

Nessus was able to verify the issue using the following URL :

http://192.168.0.21/index.php/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000

Description
The PHP install on the remote server is configured in a way that allows disclosure of potentially sensitive information to an attacker through a special URL. Such an URL triggers an Easter egg built into PHP itself.

Other such Easter eggs likely exist, but Nessus has not checked for them.

Solution
In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.

See also
http://www.0php.com/php_easter_egg.php
http://seclists.org/webappsec/2004/q4/324

Risk Factor
Medium/ CVSS Base Score: 5.0
(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Other references
OSVDB:12184

Vulnerability publication date: 2004/11/28
Plugin publication date: 2010/06/03

Plugin last modification date: 2011/03/14

Port www (8834/tcp)

Plugin ID: 10662
Web mirroring

Synopsis

Nessus crawled the remote web site.
List of Hosts

192.168.0.59
Plugin Output

The following CGI have been discovered :

Syntax : cginame (arguments [default value])

/file/upload (Filedata [])

192.168.0.54
Plugin Output

The following CGI have been discovered :

Syntax : cginame (arguments [default value])

/file/upload (Filedata [])

192.168.0.53
Plugin Output

The following CGI have been discovered :

Syntax : cginame (arguments [default value])

/file/upload (Filedata [])

192.168.0.52
Plugin Output

The following CGI have been discovered :

Syntax : cginame (arguments [default value])

/file/upload (Filedata [])

192.168.0.41
Plugin Output

The following CGI have been discovered :

Syntax : cginame (arguments [default value])

/file/upload (Filedata [])

192.168.0.33
Plugin Output

The following CGI have been discovered :

Syntax : cginame (arguments [default value])

/file/upload (Filedata [])

192.168.0.25
Plugin Output

The following CGI have been discovered :

Syntax : cginame (arguments [default value])

/file/upload (Filedata [])

192.168.0.24

Plugin Output

The following CGI have been discovered :

Syntax : cginame (arguments [default value])

/file/upload (Filedata [])

Description
This script makes a mirror of the remote web site(s) and extracts the
list of CGIs that are used by the remote host.

It is suggested that you change the number of pages to mirror in the
'Options' section of the client.

Solution
n/a

Risk Factor
None

Plugin publication date: 2001/05/04

Plugin last modification date: 2012/01/04

Port (80/tcp)

Plugin ID: 10662
Web mirroring

Synopsis

Nessus crawled the remote web site.
List of Hosts

192.168.0.40
Plugin Output

Directory index found at /
Directory index found at /ubuntu/
Directory index found at /xp/

192.168.0.21
Plugin Output

Directory index found at /php/

Description
This script makes a mirror of the remote web site(s) and extracts the list of CGIs that are used by the remote host.

It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

Solution
n/a

Risk Factor
None

Plugin publication date: 2001/05/04

Plugin last modification date: 2012/01/04

Port (0/tcp)

Plugin ID: 57436
USN-1317-1 : ghostscript vulnerabilities

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

List of Hosts

192.168.0.25

Plugin Output

- Installed package : libgs8_8.71.dfsg.1-0ubuntu5.3
Fixed package : libgs8_8.71.dfsg.1-0ubuntu5.4

Description

It was discovered that Ghostscript did not correctly handle memory allocation when parsing certain malformed JPEG-2000 images. If a user or automated system were tricked into opening a specially crafted image, an attacker could cause a denial of service and possibly execute arbitrary code with user privileges. (CVE-2008-3520)

It was discovered that Ghostscript did not correctly handle certain formatting operations when parsing JPEG-2000 images. If a user or automated system were tricked into opening a specially crafted image, an attacker could cause a denial of service and possibly execute arbitrary code with user privileges. (CVE-2008-3522)

It was discovered that Ghostscript incorrectly handled certain malformed TrueType fonts. If a user or automated system were tricked into opening a document containing a specially crafted font, an attacker could cause a denial of service and possibly execute arbitrary code with user privileges. This issue only affected Ubuntu 8.04 LTS. (CVE-2009-3743)

It was discovered that Ghostscript incorrectly handled certain malformed Type 2 fonts. If a user or automated system were tricked into opening a document containing a specially crafted font, an attacker could cause a denial of service and possibly execute arbitrary code with user privileges. This issue only affected Ubuntu 8.04 LTS. (CVE-2010-4054)

Jonathan Foote discovered that Ghostscript incorrectly handled certain malformed JPEG-2000 image files. If a user or automated system were tricked into opening a specially crafted JPEG-2000 image file, an attacker could cause Ghostscript to crash or possibly execute arbitrary code with user privileges. (CVE-2011-4516, CVE-2011-4517)

Solution

Update the affected package(s).

See also

http://www.ubuntu.com/usn/usn-1317-1/

Risk Factor

Critical/ CVSS Base Score: 10.0
(CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVE

CVE-2008-3520
CVE-2008-3522
CVE-2009-3743
CVE-2010-4054
CVE-2011-4516
CVE-2011-4517

Other references

USN:1317-1
CWE:119

Patch publication date: 2012/01/04
Plugin publication date: 2012/01/05

Plugin last modification date: 2012/01/05

Port www (80/tcp)

Plugin ID: 11229
Web Server info.php / phpinfo.php Detection

Synopsis

The remote web server contains a PHP script that is prone to an information disclosure attack.

List of Hosts

192.168.0.67

Plugin Output

Nessus discovered the following URL that calls phpinfo() :

- http://192.168.0.67/phpinfo.php

Description

Many PHP installation tutorials instruct the user to create a PHP file that calls the PHP function 'phpinfo()' for debugging purposes. Various PHP applications may also include such a file. By accessing such a file, a remote attacker can discover a large amount of information about the remote web server, including :

- The username of the user who installed php and if they are a SUDO user.

- The IP address of the host.

- The version of the operating system.

- The web server version.

- The root directory of the web server.

- Configuration information about the remote PHP installation.

Solution
Remove the affected file(s).

Risk Factor
Medium/ CVSS Base Score: 5.0
(CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

Plugin publication date: 2003/02/12

Plugin last modification date: 2011/03/15

Port www (80/tcp)

Plugin ID: 55976
Apache HTTP Server Byte Range DoS

Synopsis

The web server running on the remote host is affected by a denial of service vulnerability.
List of Hosts

192.168.0.67
Plugin Output

Nessus determined the server is unpatched and is not using any
of the suggested workarounds by making the following requests :

```
------------------- Testing for workarounds --------------------
HEAD / HTTP/1.1
Host: 192.168.0.67
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Request-Range: bytes=5-0,1-1,2-2,3-3,4-4,5-5,6-6,7-7,8-8,9-9,10-10
Range: bytes=5-0,1-1,2-2,3-3,4-4,5-5,6-6,7-7,8-8,9-9,10-10
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
```

HTTP/1.1 206 Partial Content
Date: Fri, 27 Jan 2012 23:08:21 GMT
Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
Last-Modified: Wed, 17 Mar 2010 14:08:25 GMT
ETag: "107f7-2d-481ffa5ca8840"
Accept-Ranges: bytes
Content-Length: 827
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: multipart/x-byteranges; boundary=4b78a92b2a39c1584
------------------- Testing for workarounds --------------------

------------------- Testing for patch --------------------
HEAD / HTTP/1.1
Host: 192.168.0.67
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Request-Range: bytes=0-,1-
Range: bytes=0-,1-
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

HTTP/1.1 206 Partial Content
Date: Fri, 27 Jan 2012 23:08:26 GMT
Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
Last-Modified: Wed, 17 Mar 2010 14:08:25 GMT
ETag: "107f7-2d-481ffa5ca8840"
Accept-Ranges: bytes
Content-Length: 274
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: multipart/x-byteranges; boundary=4b78a92fb1a163c41
------------------- Testing for patch --------------------

Description

The version of Apache HTTP Server running on the remote host is affected by a denial of service vulnerability. Making a series of HTTP requests with overlapping ranges in the Range or Request-Range request headers can result in memory and CPU exhaustion. A remote, unauthenticated attacker could exploit this to make the system

unresponsive.

Exploit code is publicly available and attacks have reportedly been observed in the wild.

Solution

Upgrade to Apache httpd 2.2.21 or later, or use one of the workarounds in Apache's advisories for CVE-2011-3192. Version 2.2.20 fixed the issue, but also introduced a regression.

If the host is running a web server based on Apache httpd, contact the vendor for a fix.

See also

http://archives.neohapsis.com/archives/fulldisclosure/2011-08/0203.html
http://www.gossamer-threads.com/lists/apache/dev/401638
http://www.nessus.org/u?404627ec
http://www.apache.org/dist/httpd/CHANGES_2.2.20
http://www.nessus.org/u?1538124a
http://www-01.ibm.com/support/docview.wss?uid=swg24030863

Risk Factor

High/ CVSS Base Score: 7.8
(CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:C)
CVSS Temporal Score: 6.4(CVSS2#E:F/RL:OF/RC:C)

CVE

CVE-2011-3192

Bugtraq ID

49303

Other references

OSVDB:74721
CERT:405811
EDB-ID:17696
EDB-ID:18221
IAVA:2011-A-0120
IAVA:2011-A-0130
IAVA:2011-A-0141

Vulnerability publication date: 2011/08/19
Patch publication date: 2011/08/25
Plugin publication date: 2011/08/25
Plugin last modification date: 2011/12/12

Ease of exploitability: Exploits are available

192.168.0.67

Scan Time	
Start time:	Sat Jan 28 07:01:59 2012
End time:	Sat Jan 28 07:07:38 2012

Number of vulnerabilities	
High	4
Medium	3
Low	36

Remote Host Information	
Operating System:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
NetBIOS name:	METASPLOITABLE
IP address:	192.168.0.67
MAC address:	08:00:27:b3:f9:f8

^Back

192.168.0.63

Scan Time	
Start time:	
End time:	Sat Jan 28 07:07:55 2012

Number of vulnerabilities	
High	0
Medium	0
Low	2

Remote Host Information	
MAC address:	08:00:27:a2:a6:32

^Back

192.168.0.59

Scan Time	
Start time:	Sat Jan 28 07:01:24 2012
End time:	Sat Jan 28 07:07:46 2012

Number of vulnerabilities	
High	0
Medium	4
Low	40

Remote Host Information	
Operating System:	Linux Kernel 2.6
NetBIOS name:	BT
IP address:	192.168.0.59
MAC address:	00:26:2d:91:45:56

^Back

192.168.0.54

Scan Time	
Start time:	Sat Jan 28 07:01:14 2012
End time:	Sat Jan 28 07:11:43 2012

Number of vulnerabilities	
High	0
Medium	6

Low	40

Remote Host Information	
Operating System:	Linux Kernel 2.6
NetBIOS name:	BT
IP address:	192.168.0.54
MAC address:	14:da:e9:23:0b:a4

^Back

192.168.0.53

Scan Time	
Start time:	Sat Jan 28 07:01:04 2012
End time:	Sat Jan 28 07:07:37 2012

Number of vulnerabilities	
High	0
Medium	6
Low	40

Remote Host Information	
Operating System:	Linux Kernel 2.6
NetBIOS name:	BT
IP address:	192.168.0.53
MAC address:	20:6a:8a:40:45:c8

^Back

192.168.0.52

Scan Time	
Start time:	Sat Jan 28 07:01:04 2012
End time:	Sat Jan 28 07:07:22 2012

Number of vulnerabilities	
High	0
Medium	4
Low	40

Remote Host Information

Operating System:	Linux Kernel 2.6
NetBIOS name:	BT
IP address:	192.168.0.52
MAC address:	00:26:22:52:5f:c9

^Back

192.168.0.41

Scan Time

Start time:	Sat Jan 28 07:00:39 2012
End time:	Sat Jan 28 07:07:06 2012

Number of vulnerabilities

High	0
Medium	4
Low	40

Remote Host Information

Operating System:	Linux Kernel 2.6
NetBIOS name:	BT
IP address:	192.168.0.41
MAC address:	00:23:8b:78:80:4f

^Back

192.168.0.40

Scan Time

Start time:	Sat Jan 28 07:00:39 2012
End time:	Sat Jan 28 07:03:09 2012

Number of vulnerabilities

High	0
Medium	1
Low	23

Remote Host Information

Operating System:	Linux Kernel 2.6 on Ubuntu 10.10 (maverick)
IP address:	192.168.0.40
MAC address:	10:78:d2:36:65:a4

^Back

192.168.0.33

Scan Time

Start time:	Sat Jan 28 07:00:24 2012
End time:	Sat Jan 28 07:06:49 2012

Number of vulnerabilities

High	0
Medium	6
Low	40

Remote Host Information

Operating System:	Linux Kernel 2.6
NetBIOS name:	BT
IP address:	192.168.0.33
MAC address:	00:25:64:67:3b:1d

^Back

192.168.0.25

Scan Time

Start time:	Sat Jan 28 07:00:09 2012
End time:	Sat Jan 28 07:08:12 2012

Number of vulnerabilities

High	44
Medium	30
Low	46

Remote Host Information

Operating System:	Linux Kernel 2.6.39.4 on Ubuntu 10.04
NetBIOS name:	BT
DNS name:	bt
IP address:	192.168.0.25
MAC address:	20:6a:8a:00:36:f2 78:e4:00:f8:53:a7

^Back

192.168.0.24

Scan Time

Start time:	Sat Jan 28 07:00:09 2012
End time:	Sat Jan 28 07:06:36 2012

Number of vulnerabilities

High	0
Medium	6
Low	40

Remote Host Information

Operating System:	Linux Kernel 2.6
NetBIOS name:	BT
IP address:	192.168.0.24
MAC address:	00:26:22:73:84:f3

^Back

192.168.0.23

Scan Time

Start time:	Sat Jan 28 07:00:09 2012
End time:	Sat Jan 28 07:12:51 2012

Number of vulnerabilities

High	0
Medium	4
Low	19

Remote Host

Information	
Operating System:	Linux Kernel 2.6
IP address:	192.168.0.23
MAC address:	98:4b:e1:c0:e6:b1

^Back

192.168.0.21

Scan Time	
Start time:	Sat Jan 28 07:00:04 2012
End time:	Sat Jan 28 07:04:19 2012

Number of vulnerabilities	
High	1
Medium	5
Low	36

Remote Host Information	
Operating System:	Linux Kernel 2.6
NetBIOS name:	UBUNTUVM
IP address:	192.168.0.21
MAC address:	08:00:27:f9:c1:bb

^Back