The PWNIE Awards 2024

Pwnie for Best Crypto Bug

Breach Extraction Attacks	The paper describes attacks leveraging leakage from cryptographic protocols and compromised credential-checking services, specifically Cloudflare's implementation, to reconstruct encrypted passwords on servers. It combines cryptographic insights and neural networks to guess encrypted credentials in an unprecedented manner.	@kornaropoulos
GoFetch: Breaking Constant-Time Cryptographic Implementations Using Data Memory-Dependent Prefetchers	A microarchitectural side-channel attack that exploits data memory-dependent prefetchers on the latest Apple processors to extract secret keys from constant-time cryptographic implementations.	boruchen
Blast Radius: RADIUS/UDP Considered Harmful	This significant attack targets a major protocol using a powerful, underused vector that exploits the legacy use of MD5, which lacks	nadiah

	chosen-prefix collision resistance.	

Pwnie for Best Desktop Bug

Ben Barnea's 3-episode research on Windows paths	Ben Barnea's three-part research highlights the complexity of parsing Windows paths, even for Microsoft decades after developing the code. These minor mistakes and bugs can lead to severe consequences, such as zero-click vulnerabilities in Outlook or Windows Explorer, showcasing the researcher's dedication to critical but overlooked code in Windows core.	@nachoskrnl
A Chrome 0day caused by improperly triggered audio rendering	In the current WebAudio standard, real-time audio rendering is supposed to start only after user interaction with the web page. However, a longstanding bug in Chrome allows forced real-time audio rendering without user interaction. Although this bug has existed for over ten years, it was not considered a security issue until it was exploited in last year's Tianfu Cup.	@7o8v1
Bytecode Breakdown: Unraveling Factorio's Lua Security Flaws	Daniel s b exploited a vulnerability in the Lua implementation of Factorio, enabling a malicious server to execute arbitrary code on clients. Since all clients in Factorio act as "servers" by sending inputs through the "main" server, this vulnerability affects every player.	danielsb

Pwnie for Best Mobile Bug

Operation Triangulation	Operation Triangulation, revealed by Kaspersky researchers, uncovered one of the most sophisticated attacks targeting iPhones. This attack is notable for being the first to exploit a hardware “feature” in iPhones.	¯_(ツ)_/¯

Gaining kernel code execution on an MTE-enabled Pixel 8 (CVE-2023-6241)	This research examines a vulnerability in the Arm Mali GPU that allows a malicious app to achieve arbitrary kernel code execution and gain root access on an Android phone. It demonstrates how this vulnerability can be exploited even when the Memory Tagging Extension (MTE) mitigation is enabled on the device.	@mmolgtm
That Samsung 'Galaxy A' bug chain	The bug chain can be triggered via USB, allowing code execution in the bootloader, control over Android, and leakage of secrets stored in Trustzone, such as Keystore keys. While the individual bugs aren't particularly interesting, the chain is impressive and highly impactful, affecting many devices in the Galaxy A family.	@max_r_b, @DamianoMelotti, Raphael Neveu

Pwnie for Best Song

Touch Some Grass - UWU Underground	https://x.com/uwu_underground/status/1787888869402361941	@uwu_underground
c0de - SnailLoad	c0de - SnailLoad (A Parody Song)	@lavados
The Bottom 2	Glorb - The Bottom 2 (Official Music Video)	Glorb

Pwnie for Best Priv Esc

Unplugging XHCI: An Enabling Step on the Road to VMware VM Escape	At Black Hat Asia 2024, this presentation detailed a successful VMware Workstation escape exploit from the Tianfu Cup 2023. By removing the xHCI USB controller within the virtual machine, they triggered a Use-After-Free vulnerability with a remounted USB mouse, combined with an information leak to escape VMware. This innovative approach demonstrated the power of exploit components in default configuration environments.	@vv474172261
A (registry) window to kernel memory (CVE-2023-23420)	CVE-2023-23420, discovered by j00ru, highlights three key points. First, memory corruption in Windows	mjurczyk

	Registry handling is a powerful vector due to the predictability of the in-memory registry layout. Second, in-place renames of registry keys are so incompatible with registry transactions that they had to be removed to fix this bug. Third, it demonstrates that REG_QWORD and REG_BINARY registry values can provide direct access to KERNEL memory, effectively turning regedit into a kernel memory editor.	
Windows Streaming Service UAF Used at Pwn2Own Vancouver	During the competition, Chompie exploited an improper object reference count update in the Microsoft Kernel Streaming Server (mskssrv.sys). The issue occurs when an FSContextReg object is initialized and registered, and the DispatchCleanup and DispatchClose functions are called from a process that didn't initialize or register the object, causing a use-after-free for a vtable call. Her successful exploitation earned her $15,000, though Microsoft later listed the exploit code maturity as "Unproven" despite her live demonstration.	@chompie1337

Pwnie for Best RCE

Jumpserver Preauth RCE Exploit Full Chain	JumpServer, a popular open-source PAM, helps enterprises securely control and log in to various types of assets. Lawliet and Zhiniang Peng (@edwardzpeng) exploited insecure random number logic in Python to achieve authentication bypass, resulting in Preauth RCE.	@edwardzpeng, Lawliet
“Half Measures and Full Compromise” - Chain of 3 Vulnerabilities to Pwn Exchange	This Microsoft Exchange RCE chain consists of three vulnerabilities: (1) Argument Injection to File Write, allowing a DLL to be dropped onto the file system, (2) File Read, leaking the DLL drop path from the log file, and (3) Local DLL loading vulnerability, enabling RCE. This exploit can be executed by any domain user.	Piotr Bazydlo @chudyPB
The Overlooked Pattern: CVE-2024-30080's Path to pre-auth RCE	“The Overlooked Pattern” is a critical pre-authenticated remote code execution vulnerability with a CVSS score of 9.8. Affecting all Windows versions from Server 2008 to Server 2022, and	R00t0xk0shl ?

	Windows 10 and 11, the flaw stems from a use-after-free issue triggered via an HTTP-based protocol. The vulnerable object is fully controllable, heightening the exploitation risk. Notably, the bug was discovered through an overlooked RPC client pattern.	

Pwnie for Epic Achievement

Discovery of the XZ backdoor	Andres discovered a backdoor in xz-utils while troubleshooting performance issues, more or less by accident. His attention to performance and dedication to fixing the underlying problem led to this discovery, ultimately saving a number of linux distros that had already rolled it into their dev builds.	Andres Freund
Windows Downdate: Downgrade Attacks Using Windows Updates	This research uncovered a critical flaw in Windows Updates that allows attackers to downgrade files, bypassing all verification checks and enabling privilege escalation from ring 3 (User Mode) to ring -1 (Hypervisor). This flaw also allows disabling Virtualization Based Security (VBS) and its features, even with UEFI locks. The findings, presented at Black Hat USA 2024 and DEF CON 32, show how attackers can exploit this flaw to revive old vulnerabilities and turn fixed issues into new 0-days, undermining the concept of "fully patched" Windows systems.	@_0xDeku, Alon Leviev
Flexo	This research showcases a binary unpacker operating within a "microarchitectural weird machine," using microarchitectural state and side channels instead of traditional memory and registers, making malware analysis significantly harder. The study also reveals the broader potential of these machines as computational primitives and introduces a compiler to aid in constructing advanced obfuscated computations.	Ping-Lun Wang (Carnegie Mellon University) Riccardo Paccagnella (Carnegie Mellon University) Riad S. Wahby (Carnegie Mellon University) Fraser Brown (Carnegie Mellon University)

Pwnie for Epic Fail

Lol	

Lmao even	

Pwnie for Lamest Vendor Response

Linux CVE CNA	Linux Kernel team is giving **every** bug a CVE not just the vulns. What could go wrong?	Linux Folks?
Xiaomi's Pwn2Own Infrastructure Fail	Xiaomi disabled parts of its infrastructure - including its global app store to stop pwn2own contestants from pwning.	Xiaomi
Kaspersky Antivirus	Trying to claim a bug bounty from Apple for Triangulation. Can't pay out sanctioned entities guys sorry. Sucks to suck.	Kaspersky

Pwnie for Most Innovative

Ahoi Attacks	The Ahoi attack introduces a novel method of injecting virtual interrupts into Confidential VMs (CVMs) to alter their execution state and break confidentiality, a significant departure from previous research that only used interrupts to stop TEEs. This technically challenging attack required 39 interrupts to leak/overwrite 8 bytes in a CVM.	Benedict Schlueter
TuDoor Attack: Systematically Exploring and Exploiting Logic Vulnerabilities in DNS Response Pre-processing with Malformed Packets	The TuDoor attack exploits DNS response pre-processing vulnerabilities to perform DNS cache poisoning within 1 second, significantly faster than previous methods. This research identified three new logic vulnerabilities affecting 24 mainstream DNS software and numerous routers and public DNS services, leading to the assignment of 33 CVE IDs and mitigation discussions with vendors. The findings highlight the need for standardized DNS response pre-processing to enhance security, as detailed in IEEE S&P 2024 and referenced by RFC 9520.	idealeer
Let the Cache Cache and Let the WebAssembly Assemble: Knockin' on Chrome's Shell	Exploiting Chrome's V8 JavaScript engine has become increasingly difficult with the introduction of the V8	Edouard Bochin @le_douds) Tao Yan (@Ga1ois)

	Sandbox, designed to prevent memory corruption vulnerabilities. Despite this, a novel V8 Sandbox escape technique was successfully demonstrated at Pwn2Own Vancouver 2024, breaking both V8 and the V8 Sandbox and ending Chrome's three-year undefeated streak at the competition. This new technique, which manipulates sandboxified object fields rather than relying on raw pointers, has set a new precedent in V8 exploitation and was detailed earlier this week at Black Hat.	

Pwnie for Most Underhyped Research

See No Eval: Runtime Dynamic Code Execution in Objective-C	In 2019, a CTF challenge used a technique for dynamic code execution in Objective-C, which was later detailed by CodeColorist in a 2021 blog post. Although it initially received little attention, analysis reveals that several iOS exploits have used this technique in active attacks since 2021, including FORCEDENTRY, Operation Triangulation, and BLASTPASS. It remains unclear whether threat actors used this technique before the research was published or were inspired by it.	@codecolorist
Dangerous Import: SourceForge Patches Critical Code Vulnerability	This vulnerability is in Apache Allura, which powers the popular software platform SourceForge, serving 2.6 million software downloads daily. Malicious actors could have exploited this vulnerability to fully compromise SourceForge and spread malware to millions of users via popular applications like KeePass, Apache OpenOffice, and XAMPP. Despite its potential impact, the vulnerability received little public attention.	@scryh_
Flexo	This research once again showcases a binary unpacker operating within a "microarchitectural weird machine," using microarchitectural state and side channels instead of traditional memory and registers, making malware analysis significantly harder. The study also reveals the broader potential of these machines as computational primitives and introduces a compiler to aid in constructing advanced obfuscated computations.	Ping-Lun Wang, Riccardo Paccagnella, Riad Wahby, Fraser Brown