

| Hacking Team Exploits Summary | | | | | | | |
|---|---------------------------|---------------|----------------|-----------------------|---|---|---|
| Affected Software Name | CVE | Related Info | Bug Type | Discl. Date | Link to PoC/Exploit | Link to vendor update information | |
| 0-day | Adobe Flash Player | CVE-2015-5119 | ByteArray | Use-After-Free | 7-Jul-2015 | https://wikileaks.org/hackingteam/emails/emailid/514629 | https://helpx.adobe.com/security/products/flash-player/apsa15-03.html |
| | Adobe Flash Player | CVE-2015-5122 | DisplayObject | Use-After-Free | 11-Jul-2015 | https://wikileaks.org/hackingteam/emails/emailid/45977 | https://helpx.adobe.com/security/products/flash-player/apsa15-04.html |
| | Adobe Flash Player | CVE-2015-5123 | BitmapData | Use-After-Free | 11-Jul-2015 | https://wikileaks.org/hackingteam/emails/emailid/514936 | https://helpx.adobe.com/security/products/flash-player/apsa15-04.html |
| | MS Windows Vista - 8.1 | CVE-2015-2387 | atmfd.dll | Integer Overflow | 7-Jul-2015 | | https://technet.microsoft.com/en-us/library/security/ms15-077.aspx |
| | MS Windows Vista - 8.1 | CVE-2015-2426 | atmfd.dll | OOB Write | 20-Jul-2015 | https://wikileaks.org/hackingteam/emails/emailid/974752 | https://technet.microsoft.com/en-us/library/security/ms15-078.aspx |
| MS Internet Explorer | CVE-2015-2425 | jscrip.dll | Use-After-Free | 14-Jul-2015 | https://wikileaks.org/hackingteam/emails/emailid/902517 | https://technet.microsoft.com/en-us/library/security/ms15-065.aspx | |
| ? | Adobe Flash Player | CVE-2015-3087 | | Integer Overflow | | https://wikileaks.org/hackingteam/emails/emailid/987809 | https://helpx.adobe.com/security/products/flash-player/apsb15-09.html |
| | MS Internet Explorer bug | ? | | | | https://wikileaks.org/hackingteam/emails/emailid/508630 | |
| | Android 2.3 WebKit PoC | ? | | | | https://wikileaks.org/hackingteam/emails/emailid/123973 | |
| | Android 4.0 - 4.3 Browser | CVE-2011-1202 | | Information Leak | | https://github.com/hackedteam/vector-exploit/tree/master/src/ht-webkit-Android4-src | |
| | Android 4.0 - 4.3 Browser | CVE-2012-2825 | | Arbitrary Memory Leak | | https://github.com/hackedteam/vector-exploit/tree/master/src/ht-webkit-Android4-src | |
| | Android 4.0 - 4.3 Browser | CVE-2012-2871 | | Heap Buffer Overflow | | https://github.com/hackedteam/vector-exploit/tree/master/src/ht-webkit-Android4-src | |
| Adobe Flash Player | CVE-2015-0349 | | Use-After-Free | | | https://helpx.adobe.com/security/products/flash-player/apsb15-06.html | |
| More information: | | | | | | | |
| http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-team-uses-uefi-bios-rootkit-to-keep-rce-9-agent-in-target-systems/ | | | | | | | |
| https://www.rooksecurity.com/hacking-team-malware-detection-utility/ | | | | | | | |
| http://tsyrklevich.net/2015/07/22/hacking-team-0day-market/ | | | | | | | |
| Made by: | | | | | | | |
| https://twitter.com/ax330d | | | | | | | |