Security Leftovers

By *Roy Schestowitz*
Created *25/02/2020 - 4:43pm*
Submitted by Roy Schestowitz on Tuesday 25th of February 2020 04:43:51 PM Filed under Security [1]

- **Security updates for Monday [2]**

  Security updates have been issued by Debian (libpam-radius-auth, pillow, ppp, proftpd-dfsg, and python-pysaml2), Fedora (firefox, glib2, hiredis, http-parser, libuv, mingw-openjpeg2, nghttp2, nodejs, openjpeg2, python-pillow, skopeo, and webkit2gtk3), Mageia (patch, postgresql, and systemd), Red Hat (ksh, nodejs:10, openjpeg2, python-pillow, systemd, and thunderbird), and SUSE (java-1_7_1-ibm, libsolv, libzypp, zypper, pdsh, slurm_18_08, and php53).

- **U.S. Government Says Update Chrome 80 As High-Rated Security Flaws Found [3]**

  Are you a Google Chrome user? High-rated security vulnerabilities have already been discovered in version 80 of Google Chrome. The Cybersecurity and Infrastructure Security Agency is encouraging Google users to update again just weeks after the Chrome 80 release. Here?s what you need to know.

- **OpenBSD Pwned, Patched Again: Bug is Remotely Exploitable [4] [Ed: Misleading. This is about OpenSMTPD.]**

  There?s a fresh remote code execution (RCE) vulnerability in OpenSMTPD, and by extension in OpenBSD. Yes, it feels like déjà vu all over again.

  The severity of the vulnerability, CVE-2020-8794, means that anyone running a public-facing OpenSMTPD deployments should update as soon as possible.

OpenBSD?s developers describe the issue as a ?an out of bounds read in smtpd [that] allows an attacker to inject arbitrary commands into the envelope file which are then executed as root. Separately, missing privilege revocation in smtpctl allows arbitrary commands to be run with the _smtpq group.?

- **Kali Linux explained: A pentester?s toolkit [5]**

  Kali Linux is the world's most popular offensive-security-optimized Linux distro. Maintained and managed by the fine folks at Offensive Security, Kali was born in 2006 as BackTrack Linux, but after a major refactoring in 2013 got the name Kali. What does the name mean? Well, we'll get to that.

- **Police to get right to use spyware in serious crime investigations [6]**

  The new bill, that will allow the police to use trojans or virus programmes to tap into the chats, is expected to be voted through parliament on Thursday. Home Affairs Minister Mikael Damberg says he is convinced it will lead to more convictions.

- **McAfee WebAdvisor: From XSS in a sandboxed browser extension to administrator privileges [7]**

  A while back I wrote about a bunch of vulnerabilities in McAfee WebAdvisor, a component of McAfee antivirus products which is also available as a stand-alone application. Part of the fix was adding a bunch of pages to the extension which were previously hosted on siteadvisor.com, generally a good move. However, when I looked closely I noticed a Cross-Site Scripting (XSS) vulnerability in one of these pages (CVE-2019-3670).

  Now an XSS vulnerability in a browser extension is usually very hard to exploit thanks to security mechanisms like Content Security Policy and sandboxing. These mechanisms were intact for McAfee WebAdvisor and I didn?t manage to circumvent them. Yet I still ended up with a proof of concept that demonstrated how attackers could gain local administrator privileges through this vulnerability, something that came as a huge surprise to me as well.

Security

Source URL: http://www.tuxmachines.org/node/134473

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://lwn.net/Articles/813153/rss

[3] https://www.forbes.com/sites/daveywinder/2020/02/22/google-chrome-80-security-warning-us-government-says-update-again/
[4] https://www.cbronline.com/news/openbsd-opensmtpd-qualys
[5] https://www.csoonline.com/article/3528191/kali-linux-explained-a-pentester-s-toolkit.html
[6] https://sverigesradio.se/sida/artikel.aspx?programid=2054&artikel=7410106
[7] https://palant.de/2020/02/25/mcafee-webadvisor-from-xss-in-a-sandboxed-browser-extension-to-administrator-privileges/