Security: Patches, Linux Format Special and POWER9 Problems

By *Roy Schestowitz*
Created *20/11/2020 - 5:10pm*
Submitted by Roy Schestowitz on Friday 20th of November 2020 05:10:28 PM Filed under Security [1]

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

  Security updates have been issued by CentOS (firefox), Fedora (chromium, microcode_ctl, mingw-libxml2, seamonkey, and xen), openSUSE (slurm_18_08 and tor), Oracle (thunderbird), SUSE (buildah, firefox, go1.14, go1.15, krb5, microcode_ctl, perl-DBI, podman, postgresql12, thunderbird, ucode-intel, wireshark, wpa_supplicant, and xen), and Ubuntu (firefox and phpmyadmin).

- **Cyber insecurity | Linux Format [3]**

  Each year we proclaim it?s time to learn how to hack. But why? Jonni always gets angry at the subversion of the term ?hacking? and I can understand why. Hacking is fun, as is finding out how systems work and how to get them to do things they were never meant to do.

  With open source and the Linux ecosystem there?s an abundance of hacking fun to be had, and it?s no wonder all the key tools for learning how to hack ? and actually hack ? are developed and run out of Linux systems.

  For this year?s look at the world of hacking Jonni?s introducing you to the metasploit framework. This is a playground where you can learn, explore and develop hacking skills. It?s usually paired with Kali Linux, and we?re putting these on the Linux Format DVD, which makes a welcome return.

-

IBM POWER9 CPUs Need To Flush Their L1 Cache Between Privilege Boundaries Due To New Bug[4]

CVE-2020-4788 is now public and it's not good for IBM and their POWER9 processors... This new vulnerability means these IBM processors need to be flushing their L1 data cache between privilege boundaries, similar to other recent CPU nightmares.

While IBM POWER9 allows speculatively operating on completely validated data in the L1 cache, when it comes to incompletely validated data that bad things can happen. Paired with other side channels, local users could improperly obtain data from the L1 cache.

CVE-2020-4788 was made public this morning and is now causing all stable Linux kernel series to receive the mitigation that amounts to hundreds of lines of new code. The mitigation is flushing the L1 data cache for IBM POWER9 CPUs across privilege boundaries -- both upon entering the kernel and on user accesses.

Security

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://lwn.net/Articles/837915/rss
[3] https://www.linuxformat.com//content/cyber-insecurity
[4] https://www.phoronix.com/scan.php?page=news_item&px=IBM-POWER-L1-CVE-2020-4788