Google Publishes "Leaky.Page" Showing Spectre In Action Within Web Browsers

Google has published their proof-of-concept code showing the practicality of Spectre exploits within modern web browsers' JavaScript engines. The code is out there and you can even try it for yourself on the leaky.page web-site.

Google's Leaky.Page code shows its possible to leak data at around 1kB/s when running their Chrome web browser on a Skylake CPU. The proof-of-concept code is catering to Intel Skylake CPUs while it should also work for other processors and browsers with minor modifications to the JavaScript. Google was also successful in running this Leaky.Page attack on Apple M1 ARM CPUs without any major changes.

Security updates for Friday

Security updates have been issued by Debian (mupdf and pygments), Fedora (arm-none-eabi-newlib, nodejs, python3.10, and suricata), Mageia (ansible, ceph, firejail, glib2.0, gnuplot, libcaca, mumble, openssh, postgresql, python-cryptography, python-httplib2, python-yaml, roundcube-mail, and ruby-mechanize), Scientific Linux (wpa_supplicant), Slackware (git), SUSE (crmsh, libso1v, libzypp, yast2-installation, zypper, openssl-1_0_0, python, and stunnel), and Ubuntu (pillow).

Hackers Are Swarming Microsoft Exchange [Ed: Crackers, not "hackers"]

Those Microsoft Exchange security flaws you may have heard about are really getting
pummeled. If ever there was a time for cybersecurity reporters to trot out metaphors involving phrases like “blood in the water” and maybe “deranged swarm of piranhas,” it might be right now.

[...]

Instead, ESET reports that Exchange is basically getting pillaged by close to a dozen different groups, all of which have names that sound like bad gamertags, including Tick, LuckyMouse, Calypso, Websiic, Winnti, TontoTeam, Mikroceen and DLTMiner. There are also apparently two other hacker groups that have not yet been identified. So, yeah, it’s a pretty big mess.

The hacking seems to have picked up directly after Microsoft released its patches, too, as ESET’s report states that “the day after the release of the patch? security researchers started to see many more threat actors (including Tonto Team and Mikroceen) scanning and compromising Exchange servers en masse.”

Critics fume after Github removes exploit code for Exchange vulnerabilities [5]

Github has ignited a firestorm after the Microsoft-owned code-sharing repository removed a proof-of-concept exploit for critical vulnerabilities in Microsoft Exchange that have led to as many as 100,000 server infections in recent weeks.

ProxyLogon is the name that researchers have given both to the four Exchange vulnerabilities under attack in the wild and the code that exploits them. Researchers say that Hafnium, a state-sponsored hacking group based in China, started exploiting ProxyLogon in January, and within a few weeks, five other APTs?short for advanced persistent threat groups?followed suit. To date, no fewer than 10 APTs have used ProxyLogon to target servers around the world.

Microsoft confirms Windows 10 crash issue due to March updates [6] [Ed: Even dedicated Microsoft boosters point out these issues]

Microsoft has confirmed that Windows 10 devices might crash with a Blue Screen of Death (BSOD) when printing under certain conditions after applying the March cumulative updates.

Microsoft March 2021 Patch Tuesday fixes 82 flaws, 2 zero-days [7]

Today is Microsoft’s March 2021 Patch Tuesday, and with admins already struggling with Microsoft Exchange updates and hacked servers, please be nice to your IT staff today.