Published on *Tux Machines* (http://www.tuxmachines.org)

Security: Updates, ZombieLoad, FTP, Hack.lu, Hacking SETI, and Microsoft Chaos

By *Roy Schestowitz*
Created *24/05/2019 - 2:44pm*
Submitted by Roy Schestowitz on Friday 24th of May 2019 02:44:59 PM Filed under Security [1]

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

- **ZombieLoad Mitigation Costs For Intel Haswell Xeon, Plus Overall Mitigation Impact [3]**

  > With tests over the past week following the disclosure of the Microarchitectural Data Sampling (MDS) vulnerabilities also known as "Zombieload", we've looked at the MDS mitigation costs (and now the overall Spectre/Meltdown/L1TF/MDS impact) for desktop CPUs, servers, and some laptop hardware. I've also begun doing some tests on older hardware, such as some Phoronix readers curious how well aging Intel Haswell CPUs are affected.

- **How to enhance FTP server security [4] [Ed: It just needs to be abandoned [5]]**

- **Hack.lu 2019 Call for Papers, Presentations and Workshops [6]**

  > The purpose of the hack.lu convention is to give an open and free playground where people can discuss the implication of new technologies in society. hack.lu is a balanced mix convention where technical and non-technical people can meet each others and share freely all kind of information. The convention will be held in the Grand-Duchy of Luxembourg in

> October (22-24.10.2019). The most significant new discoveries about computer network attacks and defenses, commercial security solutions, and pragmatic real world security experience will be presented in a three days series of informative tutorials. We would like to announce the opportunity to submit papers, and/or lightning talk proposals for selection by the hack.lu technical review committee. This year we will be doing workshops on the first day PM and talks of 1 hour or 30 minutes in the main track for the three days.

- **Hacking SETI [7]**

- **Legal Threats Make Powerful Phishing Lures [8]**

> On or around May 12, at least two antivirus firms began detecting booby-trapped Microsoft Word files that were sent along with some various of the following message: [...]

- **US officials say foreign election [cracking] is inevitable [9]**

> "Systems that are connected to the Internet, if they're targeted by a determined adversary with enough time and resources, they will be breached," Hickey said. "So, we need to be focusing on resilience."

- **Why a Windows flaw patched nine days ago is still spooking the Internet [10]**

> The vulnerability resides in Microsoft?s proprietary Remote Desktop Protocol, which provides a graphical interface for connecting to another computer over the Internet. Exploiting the vulnerability?which is present in older versions of Windows but not the much better secured Windows 8 and 10?requires only that an attacker send specific packets to a vulnerable RDP-enabled computer. In a testament to the severity, Microsoft took the highly unusual step of issuing patches for Windows 2003, XP, and Vista, which haven?t been supported in four, five, and seven years, respectively.

- **Serial publisher of Windows 0-days drops exploits for 2 more unfixed flaws [11]**

> In Tuesday?s disclosure, SandboxEscaper wrote that the Task Scheduler vulnerability works by exploiting a flaw in the way the Task Scheduler processes changes to discretionary access

control list permissions for an individual file. An advisory published Wednesday by US Cert confirmed that the exploit worked against both 32-bit and 64-bit versions of Windows 10.

Security

Source URL: http://www.tuxmachines.org/node/124200

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://lwn.net/Articles/789224/rss
[3] https://www.phoronix.com/scan.php?page=news_item&px=Haswell-Xeon-Zombie-Load-Ref
[4] https://searchdatacenter.techtarget.com/tip/How-to-enhance-FTP-server-security
[5] https://blog.jdpfu.com/2011/07/10/why-you-need-to-stop-using-ftp
[6] https://2019.hack.lu/blog/hack.lu-2019-call-for-papers/
[7] https://www.seti.org/hacking-seti
[8] https://krebsonsecurity.com/2019/05/legal-threats-make-powerful-phishing-lures/
[9] https://www.fifthdomain.com/critical-infrastructure/2019/05/22/us-officials-say-foreign-election-hacking-is-inevitable/
[10] https://arstechnica.com/information-technology/2019/05/why-a-windows-flaw-patched-nine-days-ago-is-still-spooking-the-internet/
[11] https://arstechnica.com/information-technology/2019/05/serial-publisher-of-windows-0days-drops-exploits-for-3-more-unfixed-flaws/