Security: Updates, MDS, WhatsApp and 'The Cloud'

By *Roy Schestowitz*
Created *14/05/2019 - 6:15pm*
Submitted by Roy Schestowitz on Tuesday 14th of May 2019 06:15:51 PM Filed under Security [1]

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

- **Understanding the MDS vulnerability: What it is, why it works and how to mitigate it** **[3]**

  MDS vulnerabilities explained in ~three minutes

- **A deeper look at the MDS vulnerability** **[4]**

  In our last post, Jon Masters offered an overview of the MDS vulnerability. In this video, Jon provides a ddeper technical explanation of the vulnerability.

- **SUSE addresses Microarchitectural Data Sampling Vulnerabilities** **[5]**

  Researchers have identified new CPU side channel information leak attacks against various microarchitectural buffers used in Intel CPUs. These attacks allows local attackers to execute code to read out portions of recently read or written data by using speculative execution. Local attackers can be on the same OS or running code on the same thread of a CPU core, which could happen for other VMs on the same physical host.
  Intel, together with hardware and operating system vendors, have worked over recent months to prepare mitigations for these vulnerabilities, also known as RIDL, Fallout and ZombieLoadAttack.

- **MDS: The Newest Speculative Execution Side-Channel Vulnerability [6] [Ed: Faked performance means no security and since there are no rules associated with this, there will be no multi-billion-dollar fines, no mass recalls etc. What an awful industry.]**

  Intel just disclosed a new speculative execution side-channel vulnerability in its processors similar to the existing Spectre/L1TF vulnerabilities. This new disclosure is called the Microarchitectural Data Sampling (MDS).

  The Microarchitectural Data Sampling vulnerability was discovered by Intel researchers and independently reported as well by external researchers and is said to be similar to existing speculative execution side channel vulnerabilities. Fortunately, some current-generation CPUs are not vulnerable and Intel says all new processors moving forward will be mitigated. For those processors affected, microcode/software updates are said to be coming.

- **Update WhatsApp now to avoid spyware installation from a single missed call [7]**

- **Update WhatsApp Now, Adobe Warning Creative Cloud Users with Older Apps, Kernels Older than 5.0.8 Are Vulnerable to Remote Code Execution, Schools in Kerala Choose Linux and MakeOpenStuff Is Launching the HestiaPi Touch Smart Thermostat [8]**

  A vulnerability in WhatsApp allows spyware to be installed from a single unanswered phone call. The Verge reports that the "spyware, developed by Israel's secretive NSO group, can be installed without trace and without the target answering the call, according to security researchers and confirmed by WhatsApp. Once installed, the spyware can turn on a phone's camera and mic, scan emails and messages, and collect the user's location data. WhatsApp is urging its 1.5 billion global users to update the app immediately to close the security hole."

- **How WhatsApp exposed its users to a spyware attack [9]**

  Facebook-owned firm confirms that a vulnerability in WhatsApp opened doors for a spyware attack that installs a malicious code on victim's smartphone...

- **Modern IT security: Sometimes caring is NOT sharing [10]**

  The last decade of technological advances has seen a race to reduce costs. Migration to virtualized systems quickly eclipsed traditional bare-metal deployments. At some point, virtualization will be out-paced by containerization. While the physical footprint of an organization?s compute resources may have been reduced, the complexity of managing those

environments certainly has not.

Back in the Stone Age of IT operations and information security, everyone?s attention was focused on the corporate datacenter and the physical machines that lived there. It was simpler to understand where security controls needed to be applied. You had one giant cable coming into the building from "the internet," so you?d throw firewalls, Information Data Leak Prevention/Detection (IDP/IDS), proxies, load balancers and other tools in-line before that channel was split to the larger corporate network. This Castle-and-Moat model of protection worked fairly well (ignoring the insider threat) for decades.

[...]

Virtualization evolved into "the cloud". TL/DR for everyone out there: the cloud is just someone else?s computer. You used to run it on your server in your datacenter. Move it "to the cloud" and it now runs on Frank?s Discount Cloud and actually sits in his basement in Peoria, Illinois. Cloud-enabled individuals and businesses to have a low-cost means to quickly deploy systems and applications. It offered benefits around high availability and other features you?d typically see deployed in Enterprise-class organizations. Instead of ordering physical boxes from your favourite retailer or OEM and having that take weeks to be delivered and weeks more to be configured and deployed, now you call up Frank (say "Hi!" to his mom while she?s down in the server room doing Frank?s laundry) and Frank can have you up and running with computing and storage resources in minutes. Cloud lets you "outsource" a lot of technology and skills you might not have in-house (or have any interest in managing yourself).

Security

Source URL: http://www.tuxmachines.org/node/123893

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://lwn.net/Articles/788373/rss
[3] https://www.redhat.com/en/blog/understanding-mds-vulnerability-what-it-why-it-works-and-how-mitigate-it
[4] https://www.redhat.com/en/blog/deeper-look-mds-vulnerability
[5] https://www.suse.com/c/suse-addresses-microarchitectural-data-sampling-vulnerabilities/
[6] https://www.phoronix.com/scan.php?page=news_item&px=Microarch-Data-Sampling
[7] https://www.theverge.com/2019/5/14/18622744/whatsapp-spyware-nso-pegasus-vulnerability
[8] https://www.linuxjournal.com/content/update-whatsapp-now-adobe-warning-creative-cloud-users-older-apps-kernels-older-508-are
[9] https://www.livemint.com/technology/tech-news/how-whatsapp-exposed-its-users-to-a-spyware-attack-1557842140163.html
[10] https://www.redhat.com/en/blog/modern-it-security-sometimes-caring-not-sharing