Security flaw in CPU’s breaks isolation between cloud containers

January 9, 2018

(https://twitter.com/intent/tweet/?url=https%3A%2F%2Fnextcloud.com%2Fblog%2Fsecurity-flaw-in-intel-cpus-breaks-isolation-between-cloud-containers%2F&via=nextclouders&hashtags=nextcloud) (https://www.facebook.com/sharer.php?u=https%3A%2F%2Fnextcloud.com%2Fblog%2Fsecurity-flaw-in-intel-cpus-breaks-isolation-between-cloud-containers%2F) (https://plus.google.com/share?url=https%3A%2F%2Fnextcloud.com%2Fblog%2Fsecurity-flaw-in-intel-cpus-breaks-isolation-between-cloud-containers%2F)

Last week, two related security flaws in CPU’s from major vendors including Intel, ARM and AMD were made public. The flaw was at least known since June 2017 but already speculated at for some months in security and development circles, like in this article by LWN on November 15 (https://lwn.net/Articles/738975/), where Corbet notes about rumors circulating around undisclosed issues. On december first, it became clear the bug would impact cloud vendors, including Amazon EC2, Microsoft Azure and Google Compute Engine. Microsoft’s Azure cloud has scheduled maintenance and reboots for January 10, a date you might notice has yet to pass. Amazon notified users about a security update coming last Friday, 4 days after The Register extensively reported on the problem. (https://www.theregister.co.uk/2018/01/02/intel_cpu_design_flaw/)

We can learn two lessons from this:

- even when major vendors follow good security policy by not trying to hide the problem but fix it, there can still be a significant window between the security (both white and black hat) community knowing about the problem and the patches rolling out;
- and second, despite advances in hardware and software, the separation between customer code and data on public clouds is not guaranteed. For highly sensitive data, a hybrid cloud approach, keeping some data simply OFF the public cloud, and encryption strategies including full end-to-end encryption, seem the prudent strategy.

The issues

With hardware becoming increasingly complex, software has been creeping in. Modern CPU’s run a lot of so called ‘microcode’, embedded code to execute complex or rarely used instructions or, in case of the now infamous Intel Management Engine, a full operating system can be embedded for the purpose of remotely managing the CPU.

This obviously provides plenty opportunity for ‘unauthorized remote management’, as in, server breaches! The inherent complexity of modern CPU’s also leads them to leak information. The current flaws, fancily dubbed *Meltdown* and *Spectre*, rely on a feature named ‘speculative execution’, where CPU’s get data from memory or even execute code before being instructed to do so to speed up execution. It turns out that this feature allows unprivileged processes to probe the content of memory even outside their security boundaries. Researchers at Google (https://googleprojectzero.blogspot.de/2018/01/reading-privileged-memory-with-side.html) even managed to demonstrate the bug using Javascript from a browser, and showed examples which allow attackers to read out passwords from memory. Another Proof of Concept showed that a process running in a KVM guest on a Intel host CPU can read host kernel memory! This risk was explained by Red Hat’s chief ARM architect, Jon Masters, who was put in charge of the efforts to deal with Spectre and Meltdown at Red Hat. He noted that (http://www.datacenterknowledge.com/manage/how-red-hat-dealing-spectre-cpu-meltdown) “You can have virtual machines attack each other or attack the hypervisor.” Thus, applications could break out of the jail and get at data running in other, supposedly isolated, hypervisors.

A long window of insecurity

How long has this been a threat? These bugs have been in Intel, ARM and to a lesser degree AMD CPU’s for over a decade. Perhaps this was known in some Intelligence or Cracker circles, perhaps not. But certainly in November last year, it had become a bit of a public secret in the security world that a major hardware bug was coming. On November 15, one of the commenters on a LWN story (https://lwn.net/Articles/738975/) nailed the problem, stating “Looks like something bad is coming. Such as mega-hole maybe in hardware that can be mitigated by hiding kernel addresses.” There were rumors of a severe hypervisor bug going around at the end of 2017 and this might be that problem. Or it is another problem…

Now nobody would complain about the process the security researchers which discovered this problem followed. When they found out in early June 2017, they contacted CPU and software vendors to enable them to develop fixes. A date was set to January 9 to release information publicly so everyone had time to apply the patches. Only minor news that hinted at the problem came out the following months. But by the years’ end, there were no fixes rolled out to any system other than Apple’s Mac OS X while the problem wasn’t so secret anymore. And on January 2, the cat was effectively let out of the bag by John Leyden and Chris Williams at The Register. (https://www.theregister.co.uk/2018/01/02/intel_cpu_design_flaw/) It took more than a week for patches on public cloud infrastructure to be applied, in some cases this still has not happened. Worse, experts note that especially the Spectre vulnerabilities are not gone yet, offshoots might rear their heads for years to come.

What does this mean if you put your data and compute in a public cloud?

Let’s summarize:

- The security of public cloud infrastructure has been compromised pretty much since the start by a hardware issue unknown to the general public
- Once discovered in mid 2017, information was leaked for months and fixes were still not applied when the public became fully aware in the first days of 2018
- And this is just one problem, rumours indicate there might be more. More importantly, history indicates that there **will be**.

Now what? Hybrid, on-premise and End-to-end encryption

We have said it many times: putting data in public clouds, intermingled with data and compute from others, in jurisdictions you have little control over, is a risk. It is a risk for security, compliance and your business as a whole.

That does not mean public clouds have no place, on the contrary. The vast majority of data produced and processed in an enterprise is only tranciently sensitive and more than safe enough on servers all over the world. Cost and convenience can be important benefits of public clouds. But some data needs more protection. From fiscal year reports to patient health data to business plans, both business sensibility and government regulation demand a far higher degree of security.

For these, on-premise or managed hybrid clouds, where all or a subset of data and compute is kept from public servers, and End-to-end encryption, which ensures servers have no access to the data they store, are the main protections.

Nextcloud is the most popular self-hosted cloud technology on the market and offers the capabilities needed to protect sensitive data while allowing companies to benefit from the cost savings of a hybrid cloud strategy. You can learn more in one of our earlier blogs on data security! (https://nextcloud.com/blog/bring-enterprise-data-back-under-control-with-nextcloud/)

We started 2018 with a tweet about how we wish everybody a year with fewer security threats. We also noted that history unfortunately teaches us that there will be many, and it is better to be prepared. We didn't expect January 1 to already be breaking news on a major vulnerability (http://pythonsweetness.tumblr.com/post/169166980422/the-mysterious-case-of-the-linux-page-table), but that is how the world turns in technology…

Start the discussion at The Nextcloud forums (https://help.nextcloud.com/t/security-flaw-in-intel-cpus-breaks-isolation-between-cloud-containers/25580)

About Nextcloud

About us
(https://nextcloud.com/about)
Community
(https://nextcloud.com/contributors)
Events
(https://nextcloud.com/events)
Jobs
(https://nextcloud.com/jobs)
Code of conduct
(https://nextcloud.com/community/code-of-conduct/)
Privacy
(https://nextcloud.com/privacy)
Legal notice
(https://nextcloud.com/impressum)

Resources

Download
(https://nextcloud.com/install)
App Store
(https://apps.nextcloud.com)
Admin manual
(https://docs.nextcloud.com/server/12/admin_manual/)
User manual
(https://docs.nextcloud.com/server/12/user_manual/)
Developer manual
(https://docs.nextcloud.com/server/12/developer_manual/)
Security
(https://nextcloud.com/security)
Code on GitHub
(https://github.com/nextcloud)

Interact

Support
(https://nextcloud.com/support)
IRC Channel

(https://webchat.freenode.net/?
channels=nextcloud)
Forums
(https://help.nextcloud.com/categories)
Demo
(https://demo.nextcloud.com)
Contact us
(https://nextcloud.com/contact)
Press center
(https://nextcloud.com/press)
Bug Tracker
(https://docs.nextcloud.com/server/12/developer_manual/bugtracker/)

Follow us

Google+
(https://plus.google.com/b/104036748063781940910/104036748063781940910/about)
Facebook
(https://www.facebook.com/Nextcloud-1032807203462807/)
LinkedIn
(https://www.linkedin.com/company/10827569/)
Instagram
(https://instagram.com/nextclouders)
Twitter
(https://twitter.com/nextclouders)
YouTube
(https://youtube.com/nextcloud)
RSS Feed
(https://nextcloud.com/blogfeed)