Threat Intelligence: Spectre and Meltdown

Published: Jan 04th, 2018

Summary

Windows, Linux and MacOS have all received critical security updates that affect how virtual memory is handled due to architectural design flaws that proof of concept code has demonstrated as the tale of dual threats, called Spectre and Meltdown. Both threats break the glass ceiling and the isolation between applications by reading privileged memory and taking advantage of data cache timing vulnerabilities and have the potential of virtual memory reads across boundaries in unknown contexts.

So far, there are three known variants of the issue affecting processors by Intel, AMD and ARM

- Variant 1: bounds check bypass (CVE-2017-5753)
- Variant 2: branch target injection (CVE-2017-5715)
- Variant 3: rogue data cache load (CVE-2017-5754)

Overview

Key Findings

- Variant 1: Proof of Concept code running in userspace can perform arbitrary reads in a region of kernel memory enabling the processor to begin executing instructions long before the branchs true execution path is known. To be able to actually use this behavior for an attack, an attacker needs to be able to cause the execution of such a vulnerable code pattern in the targeted context with an out-of-bounds index.

- Variant 2: When running with root privileges inside a KVM guest OS created using virt-manager on specific versions of distribution kernels, Proof of Concept code can read host kernel memory at a rate of around 1500 bytes/second making it possible for code in separate security contexts to influence each other's branch prediction.

- Variant 3: Proof of Concept code attempts to read kernel memory from userspace without misdirecting the control flow of kernel code by using the code pattern that was used for the previous variants, but in userspace.

Mitigation

1. Identify all dev, test and production resources running affected systems and patch accordingly from trusted vendor sites in alignment with organizational update policies.

2. Continue vigilant security monitoring of known and emerging exploits with updated SIEM analytics.

3. Leverage targeted Cyber Threat Intelligence for organizational environments.

NOTES: Official infos/security advisories of involved/affected companies

Intel	Security Advisory / Newsroom
ARM	Security Update
AMD	Security Information
Microsoft	Security Guidance / Information regarding anti-virus software / Azure Blog
Amazon	Security Bulletin
Google	Project Zero Blog / Need to know
Mozilla	Security Blog
Red Hat	Vulnerability Response
Debian	Security Tracker
Ubuntu	Knowledge Base
SUSE	Vulnerability Response
LLVM	Spectre (Variant #2) Patch
CERT	Vulnerability Note
MITRE	CVE-2017-5715 / CVE-2017-5753 / CVE-2017-5754
VMWare	Security Advisory
Citrix	Security Bulletin

Further Reading

https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html

https://meltdownattack.com/

https://meltdownattack.com/meltdown.pdf

https://spectreattack.com/spectre.pdf