Meltdown & Spectre FAQ

DISCLAIMER

This document has been prepared by Avaya CCERT. The intent of this document is to provide guideline in order to enhance a company's security posture with regards to Meltdown and Spectre vulnerabilities. This document does not guarantee that your servers or infrastructure will be impenetrable.

Q1: What are Meltdown and Spectre?

All modern processors since the mid-1990's are subject to fundamental design assumptions that make them vulnerable. Meltdown and Spectre are critical vulnerabilities that can be targeted by carefully crafted software programs that allow an attacker to bypass all CPU access-protection hardware and read secrets from Kernel and Physical System Memory.

Q2: Is it an Avaya issue?

No. It is a CPU hardware issue that the industry will address by patching. Avaya is "downstream" in the supply-chain: from CPU vendors, Kernel vendors, Operating System vendors, PC and server vendors. Avaya will be able to test it and provide performance guidelines to customers, only when an "upstream" supplier provides a patch.

Q3: What are differences between Meltdown and Spectre?

The "Meltdown" exploit exposes arbitrary Privileged Operating System Kernel Data and user-space data. It is effective against Intel Processors. Meltdown can be patched, but at a performance cost.

The "Spectre" exploit exposes arbitrary user-space data (but not Kernel data). It is effective against Intel, AMD, or ARM CPU's. Patches for Spectre will be made available but it is harder to block.

Q4: How do they work?

The issue doesn't result from badly written computer code or a software bug. Instead, the problem comes down to the way the chips are intentionally designed to perform speculative execution prior to applying access permissions. First, malware would have to be installed on or sent to the system or end user apps put in place that contain malware. It would then trick the CPU into executing forbidden reads during speculative microcode execution and revealing the read value via fine-grained timing measurements

on legitimate information left in the cache. Security experts refer to these sorts of incursions as side-channel attacks, because they access information not by direct access, but by observing side-effects of it being used speculatively by a legitimate process on the computer.
It's important to note that these are vulnerabilities that make information extraction possible but malicious action isn't expected to cause applications to crash or to cease working as designed.

Q5: What is the Industry risk rating for the Meltdown and Spectre-related Common Vulnerabilities and Exposures (CVEs)?

Since the initial posting (4 January 2018), the National Vulnerability Database (NVD) has reassessed the CVSSv3 base score for each CVE from High to Medium.

- CVE-2017-5753 https://nvd.nist.gov/vuln/detail/CVE-2017-5753 CVSSv3 Base: 5.6 Medium
- CVE-2017-5715 https://nvd.nist.gov/vuln/detail/CVE-2017-5715 CVSSv3 Base: 5.6 Medium
- CVE-2017-5754 https://nvd.nist.gov/vuln/detail/CVE-2017-5754 CVSSv3 Base: 5.6 Medium

Q6: What systems are impacted?

All Manufacturers' Systems and Devices including those using Linux, OS X, iOS, Android, or Windows are impacted. Meltdown and Spectre may exploit any CPU supporting speculative execution.

Q7: How do I know/determine if my Avaya products are exposed and what remediation actions are required?

Most Avaya products running on modern CPUs are exposed, however in order to exploit these vulnerabilities, the malicious code must be installed and be running on the CPU. Avaya Best Practices recommends installing all UC and CC servers in the Data Center, behind multiple layers of firewalls, access controls and Intrusion Detection/Prevention Systems. Also, Avaya does not support 3rd party applications installations on the same CPU, but that does not prevent malicious users from attempting it, especially in the Cloud implementations.

Q8: How do attackers find a vulnerable system?

Vulnerable systems are found by scanning a network, determining systems that use impacted Operating Systems and chips and observing that patches

have not been applied, or by directly attacking any and all systems hoping to find a susceptible target.

Q9: **Has anyone been hacked via these flaws?**

As of this writing, we are unaware of any successful and widely publicized Meltdown or Spectre attacks. There is at least one "in the wild" executable file containing an example of the exploit that has been blocked by an Antivirus program. There are also working code examples published in a research paper. Now that the details of the vulnerabilities are publicly available, the chances of hackers using them in a wide variety of attacks are much higher.

Q10: How can these exploits be prevented?

Promptly install patches and updated versions of application software that address the vulnerability as Avaya and other vendors issue them. Following Security Best Practices also makes it more difficult for hackers to inject executable code into your systems.

Q11: Is there a performance impact?

Industry estimates indicate patched systems could have performance impacts of up to ~30%, which can only be determined by testing. Solutions that are running at higher levels of CPU Occupancy are more likely to demonstrate performance impacts due to patching.
Avaya will provide guidance to address any potential performance impacts due to patches that are provided.

Q12: Can an attack be detected?

On systems built to execute end-user apps, the attack just looks like another legitimate application. The attack leaves no trace.

Q13: If I've applied a patch for Meltdown and Spectre is that enough?

The industry is working on patches at every level in the compute hierarchy including microcode, firmware, hypervisor, operating system, compiler, browser, application, and system image. Ultimately, vendors will need to determine what level of patching is appropriate to safeguard their products from exploit. Only apply legitimate, approved, and tested patches.

Q14: How is Avaya responding (so far)?

Avaya Security Advisories (ASA's) are published on support.avaya.com/security, and internal Avaya teams are actively analyzing

the stream of fixes that are being made available to the industry by firmware, hypervisor, operating system, browser, and tools vendors. Avaya will continue to work these security issues according to published lifecycle and security vulnerability support policies. We are working closely with our partners to address these vulnerability issues as soon as possible.

Q15: Where can I find more information?

Avaya will continue to update security advisories at support.avaya.com/security.

Q16: When will this be "over"?

Avaya cannot make any predictions or commitments about specific releases of Avaya product being addressed in any particular timeframe or in any particular way. Avaya is testing available patches and will provide guidance when actionable information becomes available.

Avaya Security Advisories are available on support.avaya.com/security for available patches or any future updates.

Additional information can also be found on web sites for specific chip vendors and Operating Systems.

About Avaya

Avaya enables the mission critical, real-time communication applications of the world's most important operations. As a global leader in delivering superior communications experiences, Avaya provides the most complete portfolio of software and services for contact center and unified communications — offered on premises, in the cloud, or a hybrid. Today's digital world requires communications enablement, and no other company is better positioned to do this than Avaya. For more information, please visit www.avaya.com.