11 May, 2018

RE: Recent Potential CPU Vulnerabilities: Meltdown and Spectre

Meltdown and Spectre are recently disclosed security vulnerabilities that may affect nearly all CPUs shipped in the last decade (Intel, AMD, etc.) and the Operating Systems that run on those CPUs (Windows, Linux, MacOS, etc.). Mitigation is largely being provided by patching and updating software and firmware to reduce the likelihood of exploitation. These patches may have side effects to certain workloads unless properly tailored.

CVEs currently under investigation include, but are not limited to:

- CVE-2017-5753 https://nvd.nist.gov/vuln/detail/CVE-2017-5753
- CVE-2017-5715 https://nvd.nist.gov/vuln/detail/CVE-2017-5715
- CVE-2017-5754 https://nvd.nist.gov/vuln/detail/CVE-2017-5754

Note: Since the above CVE's were initially posted (1/4/2018), NVD has reassessed the CVSSv3 base score for each from High to Medium. Avaya has modified the associated Avaya Security Advisories accordingly.

UPDATE: The Avaya team has a created an FAQ document. Click HERE to access the FAQ.

Action: Please contact your Avaya Sales or Services point of contact for additional information. Also continue to visit the Avaya Support Website and Avaya Product Security for additional information as it becomes available, and to sign up for E-Notifications for additional information alerts.

Sincerely,

Avaya Security Team