AppGate Security Advisory

ID: 2018-01-001

First Published: January 8, 2018

Title: CPU vulnerability: Meltdown and Spectre

Summary

Two major CPU vulnerabilities, Spectre [1] and Meltdown [2] were publicized on January 3, 2018. The vulnerabilities are significant because a user (or hacker) could capture data from processes that a user should not normally have access to. Such data can include password, encryption keys etc.

There are no known "in the wild" exploits yet, although researchers have been able to fabricate working Proofs-Of-Concept to exploit the vulnerabilities. Local access to a shell/terminal is required for this exploit. It does not appear possible for an attacker to exploit this vulnerability remotely.

Severity: Low

This vulnerability can only be exploited by a malicious user who already has local (shell) access to the AppGate SDP or AppGate (Classic) appliance. This access should be strictly limited.

CVEs

CVE-2017-5753 hw: cpu: speculative execution bounds-check bypass
CVE-2017-5715 hw: cpu: speculative execution branch target injection
CVE-2017-5754 hw: cpu: speculative execution permission faults handling

Affected Products

We are actively investigating the impact to AppGate SDP and AppGate Classic. These vulnerabilities affects all modern Intel Processors. All versions of AppGate SDP and all supported versions of AppGate (Classic) run on physical or virtual appliances with modern Intel CPUs, and are therefore vulnerable. A local authenticated user on a terminal or shell could potentially exploit the vulnerability. To mitigate this vulnerability, limit terminal and shell access to these machines as much as possible. Only explicitly permitted users should have access to an AppGate appliance's shell, and we recommend requiring multi-factor authentication for such access.

Cyxtera is actively investigating the forthcoming Operating System patches, and will provide further instructions about how to apply these to AppGate SDP (based on Ubuntu) and AppGate Classic (based on Open Indiana) once available.

[1] https://spectreattack.com/spectre.pdf
[2] https://meltdownattack.com/meltdown.pdf
[3] https://googleprojectzero.blogspot.se/2018/01/reading-privileged-memory-with-side.html