AppGate Security Advisory

ID: 2018-01-001

First Published: January 8, 2018

Last Revised: January 23, 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 malicious user process could capture data from processes that a user process 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

From the perspective of the AppGate SDP Controller or Gateway, or AppGate Classic server, 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 to a defined set of users, and should include MFA.

From the perspective of the AppGate SDP and AppGate Classic clients, this vulnerability is not significantly different from other malware running on a user's device. Malicious software on a user's device may perform keystroke monitoring, obtain the AppGate device onboarding cookie, or dump memory. We recommend that AppGate SDP and Classic user access policies include Multi-Factor Authentication, as well as other contextual attributes such as geolocation, network, etc.

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

AppGate SDP Controller and Gateway; AppGate Classic Server:

All versions of AppGate SDP and all currently supported versions of AppGate (Classic) run on physical or virtual appliances with modern Intel CPUs, and are therefore vulnerable to these exploits. 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.

Product Updates:

AppGate SDP: Cyxtera Engineering is waiting for a stable patch release of the Ubuntu operating system that contains kernel and microcode fixes for Meltdown and Spectre. As of January 22, the Ubuntu release intended to remediate the Spectre issue was reverted, since the Intel microcode introduced system instability issues. Once a stable and supported version of Ubuntu is available, Cyxtera plans to release an updated version of the AppGate SDP server.

AppGate Classic: Cyxtera Engineering waiting for an updated release of the Open Indiana operating system, on which AppGate Classic is built. Once this patch is available, Cyxtera plans to release an updated version of the AppGate Classic server.

AppGate SDP and AppGate Classic Clients:

Clients running on Intel or AMD chips are potentially vulnerable. Customers should patch their users' operating systems to address this issue. No changes to the AppGate SDP or AppGate Classic client are needed to address this; it must be remedied within the OS.

[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