AppGate SDP
AppGate Classic
Security Advisory

ID: 2018-01-0001

First published	2018-01-08
Last updated	2018-07-12

Title

CPU vulnerability: Meltdown and Spectre

Summary

Two major CPU vulnerabilities, Spectre [1] and Meltdown [2] were first publicized on 2018-01-03.

See **Appendix** for details.

Severity

Low

Products Affected

AppGate SDP appliance versions before 3.3.3 run on appliances with modern CPUs are affected.

AppGate Classic server all versions run on appliances with modern CPUs are affected.

AppGate SDP Clients and AppGate Classic clients all versions running on modern CPUs are potentially vulnerable.

Suggested Action

Upgrade AppGate SDP appliances to version 3.3.3 and above. For clients, apply relevant host operating systems patches.

Workaround and Mitigations

Limit terminal and shell access to AppGate SDP and AppGate Classic servers as much as possible. Only explicitly permitted users should have access to an AppGate appliance’s shell and use multi-factor authentication for such access.

Appendix

Introduction

Two major CPU vulnerabilities, Spectre [1] and Meltdown [2] were first 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 widespread “in the wild” exploits, 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.

Impact

From the perspective of the AppGate SDP Controller or Gateway, or AppGate Classic server, t his 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.

Relevant 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:

As of March 9, 2018, Cyxtera has released a patched version of the AppGate SDP appliance, version 3.3.3. This release includes and updated Ubuntu operating system with kernel and microcode fixes for Meltdown and Spectre. This is available from the **AppGate SDP download center**. These fixes will be included in all future releases of the AppGate SDP platform.

Due to Ubuntu changes in how the processors handle instructions, customers can expect minor degradation in AppGate SDP appliance performance impact as follows:

Gateway: Maximum throughput test on a 10Gb/s network

- Single User - using 1 vCPU on Gateway
  - Upload performance reduced by 21% to 1.43Gb/s
  - Download performance reduced by 22% to 1.50Gb/s
- Multi User (24) – using 6 vCPU on Gateway (Note that CPU load is decreased by 3%)
  - Upload performance reduced by 17% to 5.04Gb/s
  - Download performance reduced by 23% to 5.86Gb/s
- Multi User (24) – using 40 vCPU (Note that CPU load is decreased by 1%)
  - Upload performance unchanged at 8.96Gb/s
  - Download performance unchanged at 8.87Gb/s

Controller: average login time for 10,000 users on a machine with excess CPU capacity

- Light load – 5 parallel login processes: 12% better at 176 milliseconds
- Medium load - 45 parallel login processes: 5% worse at 548 milliseconds
- Heavy load- 100 parallel login processes: 14% worse at 1353 milliseconds

AppGate Classic:

Cyxtera is 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 Clients; 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