Product Support Notice

© 2018 Avaya Inc. All Rights Reserved.

PSN #	PSN027077u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 14-Dec-18. This is Issue #02, published date: 21-Dec-18. Severity/risk level Medium Urgency When convenient

Name of problem: PSN027077u – Avaya Aura® Appliance Virtualization Platform Utilities L1 Terminal Fault (L1TF) vulnerabilities

Products affected

Avaya Aura® Appliance Virtualization Platform Utilities, Release 8.0.x

Problem description

A new industry-wide issue was found in the way many modern microprocessor designs have implemented speculative execution of instructions (a commonly used performance optimization). This latest speculative execution side channel cache timing vulnerability is called L1 Terminal Fault (L1TF). There are three varieties of L1TF that have been identified. Each variety of L1TF could potentially allow unauthorized disclosure of information residing in the L1 data cache, a small pool of memory within each processor core designed to store information about what the processor core is most likely to do next.

Resolution

Avaya Aura® Appliance Virtualization Platform Utilities (AVPU) 8.0.0 will require an upgrade to 8.0.1 for mitigation.

Note: PSNs for individual Product Applications deployed on AVP should also be reviewed for mitigation information. Refer to PSN020369u for links to individual Avaya Aura application PSNs.

- Linux Kernel: includes RHEL (Linux) kernel mitigation.
- Intel Microcode: Avaya Aura® Appliance Virtualization Platform (AVP) 7.1.3.2 and 8.0.1 include microcode mitigation for CSR1 (Common Server Release 1 – 7.1.3.2 ONLY: HP DL360 G7 and Dell R610), CSR2 (Common Server Release 2: HP DL360p G8 and Dell R620), CSR3 (Common Server Release 3: HP DL360 G9 and Dell R630), ACP 100 Series Servers - ACP120 (Dell R640) and S8300E. AVP 8.x is not supported on Common Server Release 1. Intel has not released a microcode update for the S8300D. Avaya will also provide microcode mitigation in server BIOS updates available at a future date. Customers providing their own servers for virtualized platforms must acquire BIOS updates/mitigation directly from their server vendors.
- Hypervisor: Avaya Aura® Appliance Virtualization Platform (AVP) 7.1.3.2 and 8.0.1 include VMware ESXi mitigation. Customers providing their own virtualized platform must acquire hypervisor mitigation directly from their hypervisor vendor.
    - **IMPORTANT**: There are two attack vectors addressed by VMware ESXi mitigation:
        - Sequential-Context attack vector mitigation is enabled by default and does not impose a significant performance impact.
        - Concurrent-context attack vector mitigation is not enabled by default. It requires manual intervention to enable the ESXi Side-Channel-Aware Scheduler. **Enablement of this feature may result in non-trivial performance impact and is not enabled by default**. Please see VMware KB article: VMware response to 'L1 Terminal Fault - VMM' (L1TF - VMM) Speculative-Execution vulnerability in Intel processors for vSphere: CVE-2018-3646 (55806)
        - **NOTE:** The S8300D platform for Communication Manager Survivable Remote (including Branch Session Manager) does not use Hyperthreading, so the Concurrent-Context attack vector mitigation will not have any additional performance impact). This is NOT true with the S8300E platform.

.

In AVPU testing, the Linux Kernel and Intel Microcode mitigation fixes have been shown to have a negligible impact to product performance.

NOTE: For information on L1TF mitigation refer to PSN020369u.

- In order to help mitigate the L1TF Vulnerabilities, the processor manufacturers and operating system developers provide software patches to their products. These are patches to the processors, hypervisors, and operating systems that the Avaya solutions utilize (they are not patches applied to the Avaya developed components of the solutions).

© 2018 Avaya Inc. All Rights Reserved.

- Once these patches are received by Avaya, they are tested with the applicable Avaya solutions to characterize any impact on the performance of the Avaya solutions. The objective of the testing is to reaffirm product/solution functionality and to observe the performance of the Avaya solutions in conjunction with the patches using typical operating parameters.

- Avaya is reliant on our suppliers to validate the effectiveness of their respective Speculative Execution Vulnerability patches.

- The customer should be aware that implementing these patches may result in performance degradation and that results may vary to some degree for each deployment. The customer is responsible for implementing the patches, and for the results obtained from such patches.

Once AVPU is activated and AVPU is rebooted, the security mitigation is enabled by default.
The command "kernel_opts.sh status", executed from the AVPU Command Line Interface (CLI/bash), can be used to determine what kernel mitigation is currently enabled or disabled.
This will show both Spectre/Meltdown and L1TF mitigation status.
The kernel_opts.sh enable/disable is only applicable for Spectre/Meltdown kernel mitigation, and cannot be used to disable the L1TF kernel mitigation. L1TF kernel mitigation can only be disabled by deactivating 8.0.1.

Workaround or alternative remediation

n/a

Remarks

Issue 1 – Dec 14, 2018

Issue 2 – Dec 21, 2018 – updated kernel_opts to kernel_opts.sh

Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

Backup before applying the patch.

Always.

Download

Refer to PCN 2064S Supplement 4 and PCN2081S Supplement 1.

Patch install instructions

Service-interrupting?

Refer to PCN 2064S Supplement 4 and PCN2081S Supplement 1. Yes

Verification

Refer to PCN 2064S Supplement 4 and PCN2081S Supplement 1.

Failure

Refer to PCN 2064S Supplement 4 and PCN2081S Supplement 1.

Patch uninstall instructions

Refer to PCN 2064S Supplement 4 and PCN2081S Supplement 1.

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks

Avaya uses the Common Vulnerability Scoring System version 3 (CVSSv3) base score and metrics as reported by the vendor for the affected component(s) or by the National Institute of Standards and Technology in the National Vulnerability Database. In some cases, such as where CVSS information is not available from the vendor or NIST, Avaya will calculate the CVSSv3 base score and metrics. Customers are encouraged to calculate the Temporal and Environmental CVSSv3 scores to determine how the vulnerability could affect their specific implementation or environment. For more information on CVSS and how the score is calculated, see Common Vulnerability Scoring System v3.0: Specification Document

Vulnerability	CVSSv3 Base Score	CVSSv3 Metrics
CVE-2018-3615	6.4 (Medium)	CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:N

© 2018 Avaya Inc. All Rights Reserved.

CVE-2018-3620	5.6 (Medium)	CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N
CVE-2018-3646	5.6 (Medium)	CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N

Please also reference ASA-2018-249.

Avaya Security Vulnerability Classification

High

Mitigation

N/A

For additional support, contact your Authorized Service Provider. Depending on your coverage entitlements, additional support may incur charges. Support is provided per your warranty or service contract terms unless otherwise specified.

Avaya Support Contact	Telephone
U.S. Remote Technical Services – Enterprise	800-242-2121
U.S. Remote Technical Services – Small Medium Enterprise	800-628-2888
U.S. Remote Technical Services – BusinessPartners for Enterprise Product	877-295-0099
BusinessPartners for Small Medium Product	Please contact your distributor.
Canada	800-387-4268
Caribbean and Latin America	786-331-0860
Europe, Middle East, and Africa	36-1238-8334
Asia Pacific	65-6872-8686

Disclaimer: ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED "AS IS". AVAYA INC., ON BEHALF OF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES (HEREINAFTER COLLECTIVELY REFERRED TO AS "AVAYA"), DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE STEPS RECOMMENDED WILL ELIMINATE SECURITY OR VIRUS THREATS TO CUSTOMERS' SYSTEMS. IN NO EVENT SHALL AVAYA BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE INFORMATION OR RECOMMENDED ACTIONS PROVIDED HEREIN, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE INFORMATION PROVIDED HERE DOES NOT AFFECT THE SUPPORT AGREEMENTS IN PLACE FOR AVAYA PRODUCTS. SUPPORT FOR AVAYA PRODUCTS CONTINUES TO BE EXECUTED AS PER EXISTING AGREEMENTS WITH AVAYA.

All trademarks identified by ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc.
All other trademarks are the property of their respective owners.