Product Support Notice

© 2018 Avaya Inc. All Rights Reserved.

PSN #	PSN020346u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 07-May-18. This is Issue #05, published date: 01-Oct-18.	Severity/risk level	Medium	Urgency	When convenient

Name of problem PSN020346u - Avaya Aura® Meltdown and Spectre vulnerabilities.

Products affected

Avaya Aura® Appliance Virtualization Platform, Releases 7.0.x – 7.1.x, 8.0
Avaya Aura® AVP Utilities 8.0
Avaya Aura® Application Enablement Services, Releases 6.3.x – 7.1.x, 8.0
Avaya Aura® Communication Manager, Releases 6.3.x - 7.1.x, 8.0
Avaya Aura® Media Server, Releases 7.8.x
Avaya Aura® Presence Services, Releases 6.2.x – 7.1.x
Avaya Aura® Session Manager, Releases 6.3.x - 7.1.x, 8.0
Avaya Aura® System Manager, Releases 6.3.x - 7.1.x, 8.0
Avaya Aura® Utility Services, Releases 6.3.x – 7.1.x
Avaya Aura® WebLM
Common Server R3 (HPE DL20/DL360/380 G9)
Common Server R3 (Dell R630)
Common Server R2 (HPE DL360p/380p G8)
Common Server R2 Dell R620
Common Server R1 (HPE DL360/380 G7)

Problem description

An industry-wide issue was found in the way many modern microprocessor designs have implemented speculative execution of instructions (a commonly used performance optimization). There are three primary variants of the issue which differ in the way the speculative execution can be exploited. These exploitations/vulnerabilities are commonly referred to as Meltdown and Spectre.

Resolution

- In order to mitigate the Meltdown and Spectre vulnerabilities, the processor manufacturers and operating system developers will need to provide software patches to their products. These are patches to the processors and operating systems, not to Avaya products.
- Once these patches are received by Avaya, Avaya will test these patches with the applicable Avaya products to determine what, if any, impact these patches will have on the performance of the Avaya product.
- Avaya is reliant on our Suppliers to validate the effectiveness of their respective Meltdown and Spectre vulnerability patches.
- Avaya's test effort is targeted towards reaffirming product/solution functionality and performance associated with the deployment of these patches.
- The customer is responsible for implementing, and the results obtained from, such patches.
- The customer should be aware that implementing these patches may result in performance degradation.

For detail on Meltdown and Spectre mitigation for Avaya Aura® products refer to the following product specific PSNs/PCNs:

- Avaya Aura® Appliance Virtualization Platform Meltdown and Spectre PSN027063u
  - Review Common Server PSN027066u & PSN027068u as well
- Avaya Aura® AVP Utilities 8.0 PCN2079S
- Avaya Aura® Application Enablement Services Meltdown and Spectre PSN020352u
  - Review Appliance Virtualization Platform Meltdown and Spectre PSN027063u as well
  - Review Common Server PSN027066u & PSN027068u as well
- Avaya Aura® Communication Manager Meltdown and Spectre PSN020347u
  - Review Communication Manager Kernel Service Pack 7.1.3 PCN2075Su supplement 1 as well

    - Review Appliance Virtualization Platform Meltdown and Spectre PSN027063u as well
    - Review Common Server PSN027066u & PSN027068u as well
- Avaya Aura® Media Server Meltdown and Spectre PSN020356u
    - Review Common Server PSN027066u & PSN027068u as well
- Avaya Aura® Presence Services Meltdown and Spectre PSN020353u (includes Avaya Breeze® as well)
- Avaya Aura® Session Manager Meltdown and Spectre PSN020349u
    - Review Appliance Virtualization Platform Meltdown and Spectre PSN027063u as well
    - Review Common Server PSN027066u & PSN027068u as well
- Avaya Aura® System Manager and WebLM Meltdown and Spectre PSN004811u
    - Review Appliance Virtualization Platform Meltdown and Spectre PSN027063u as well
    - Review Common Server PSN027066u & PSN027068u as well
- Avaya Aura® Utility Services Meltdown and Spectre PSN027065u
    - Review Common Server PSN027066u & PSN027068u as well
- Common Server R3 (HPE DL20/DL360/380 G9) and R2 (DL360p/380p G8) Meltdown and Spectre PSN027066u
- Common Server R3 (Dell R630) Meltdown and Spectre PSN027068u
- Common Server R2 (Dell R620) Meltdown and Spectre PSN027069u.
- Common Server R1 (HPE DL360/380 G7) Meltdown and Spectre PSN027067u.

Workaround or alternative remediation

n/a

Remarks

Issue 3 - added Avaya Aura® Media Server PSN link. Clarified Common Server bullet.

Issue 4 – added Common Server R3 Dell R630

Issue 5 – Updated for 8.0, added Common Server R2 Dell R620

Issue 6 – Updated for Common Server R1 HPE DL360 G7

Patch Notes

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

Backup before applying the patch

See product PSNs listed for product specific information.

Download

See product PSNs listed for product specific information.

Patch install instructions

Service-interrupting?

See product PSNs listed for product specific information. Yes

Verification

See product PSNs listed for product specific information.

Failure

See product PSNs listed for product specific information.

Patch uninstall instructions

See product PSNs listed for product specific information.

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

© 2018 Avaya Inc. All Rights Reserved.

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-2017-5753	5.6 (Medium)	CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N
CVE-2017-5715	5.6 (Medium)	CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N
CVE-2017-5754	5.6 (Medium)	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N

Avaya Security Vulnerability Classification

Medium

Mitigation

See product specific PSNs above.

If you require further information or assistance please contact your Authorized Service Provider, or visit support.avaya.com. There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms unless otherwise specified in the Avaya support Terms of Use.

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.