Product Support Notice

© 2018 Avaya Inc. All Rights Reserved.

PSN #	PSN020353u

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

Original publication date: 07-May-18. This is Issue #02, published date: 07-May-18.

Severity/risk level	Medium	Urgency	When convenient

Name of problem	Avaya Breeze® Platform and Presence Services Meltdown and Spectre vulnerabilities.

Products affected

Avaya Breeze® Platform, Releases 3.1.x – 3.4.x

Avaya Aura® Presence Services, Releases 7.0.x – 7.1.x

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

Breeze requires an upgrade to 3.4.0.1 for full mitigation.
Presence Services requires an upgrade to 7.1.2 Patch 3 for full mitigation. Note that Presence Services mitigation is via the Breeze Platform, and 7.1.2 Patch 3 is required for compatiblity with Breeze 3.4.0.1.

Breeze includes the following mitigation:

- Linux Kernel: Breeze 3.4.0.1 and later releases include Linux kernel mitigation.
- Intel Microcode: Avaya will provide microcode mitigation in server BIOS updates available at a future date. Customers providing their own servers must acquire BIOS updates/mitigation directly from their server vendors.
- Hypervisor: Customers providing their own virtualized platform must acquire hypervisor mitigation directly from their hypervisor vendor.

- 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.

Breeze 3.4.0.1 and higher releases allow kernel mitigation to be enabled and disabled. The mitigation is enabled by default. The mitigation can be disabled and re-enabled using the kernel_opts command from the Breeze Command Line Interface (CLI):
kernel_opts disable
kernel_opts enable

The command "kernel_opts status" can be used to determine whether kernel mitigation is currently enabled or disabled.

Note that the kernel mitigation is enabled by default, meaning when 3.4.0.1 is initially installed the mitigation is enabled. Also note that some CPU occupancy degradation might occur even with the kernel mitigation disabled:
https://access.redhat.com/articles/3311301

Breeze CPU occupancy degradation with the kernel mitigation enabled is negligible, but customers should be aware that implmenting the mitigation may result in performance degradation. The customer is responsible for assessing the nature of each specific Breeze installation, gauging the possibility of exposure of that system to the Meltdown and Spectre vulnerabilities, and making the choice to enable or disable the mitigation and the associated performance implications.

Workaround or alternative remediation

n/a

Remarks

n/a

Patch Notes

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

Backup before applying the patch

Refer to Breeze PCN2077Su and Presence Services PSN020306u for more information.

Download

Refer to Breeze PCN2077Su and Presence Services PSN020306u for more information.

Patch install instructions

Service-interrupting?

Refer to Breeze PCN2077Su and Presence Services PSN020306u for more information. Yes

Verification

Refer to Breeze PCN2077Su and Presence Services PSN020306u for more information.

Failure

Refer to Breeze PCN2077Su and Presence Services PSN020306u for more information.

Patch uninstall instructions

Refer to Breeze PCN2077Su and Presence Services PSN020306u for more 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 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

n/a

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

© 2018 Avaya Inc. All Rights Reserved.

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.

© 2018 Avaya Inc. All Rights Reserved.