Product Support Notice

© 2019 Avaya Inc. All Rights Reserved.

PSN # PSN005158u

Original publication date: 03 April 2018. This is Issue #3, published date: 25 October 2019. | Severity/risk level | Medium | Urgency | When convenient

Name of problem

Spectre / Meltdown Vulnerabilities on CS1000

Products affected

CS1000 CPP4, CPPM, CPMG, CPDC, COTS 2 and Common Server R1/R2/R3 machines

Problem description

This document is updated in October 2019 to provide info on available fixes and share a status update on new flaws related to the speculative execution of CPU instructions.

Speculative execution of CPU instructions can lead to data leakage in case of different CS1000 servers. This is a medium priority issue for CS1000. Affected and suspected CS1000 platforms are as follows.

In case of CS1000 VxWorks-based machines, use of the discussed flaws is meaningless because of the system architecture. Thus a mitigation is only required for Linux-based machines.

Platform	Status	Notes
CPP4	Not Applicable	CPP4 is a VxWorks-based Call Server, so is not applicable.
CPPM - Call Server only	Not Applicable	CPPM is a VxWorks-based Call Server, so is not applicable.
CPPM - Co-Res Call Server and Signalling Server	Not on Intel List of Affected CPUs	Kernel update for a partial mitigation against potential vulnerabilities
CPMG (CP part)	Not on Intel List of Affected CPUs	Kernel update for a partial mitigation against potential vulnerabilities
CPDC	Affected	Kernel update for a mitigation
IBM x3350	Affected	Kernel update for a partial mitigation
Dell R300	Affected	Kernel update for a partial mitigation
HP DL360 Gen7 (Common Server R1)	Affected	Kernel + microcode updates for a mitigation
HP DL360 Gen8 (Common Server R2)	Affected	Kernel + microcode updates for a mitigation
HP DL360 Gen9 (Common Server R3)	Affected	Kernel + microcode updates for a mitigation
MGC/ MGXPEC / CPMG (MGC part)	Not affected	-
MC32S / MC32 / Miran	Not affected	-

For more information on responses provided by different CPU vendors, please check the following advisories:

https://www.amd.com/en/corporate/product-security
https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00088.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00115.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00161.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00233.html

Resolution

Available fixes

A summary on fixed / open flaws related to the speculative execution of CPU instructions can be found in the following table.

CVE	Flaw	CS1000 Linux Base for Non-CSR3 machines	CS1000 amsx64 load for Non-CSR3	Any CS1000 CSR3 platform
CVE-2017-5715	BTI: Branch Target Injection (Spectre, V2)	Fixed for CSR1/CSR2 only	Fixed for CSR1/CSR2 only	Fixed
CVE-2017-5753	BCB: Bounds Check Bypass (Spectre, V1)	Fixed	Fixed	Fixed
CVE-2017-5754	RDCL: Rogue Data Cache Load (Spectre, V3 / Meltdown)	No fixes expected[3]	Fixed	Fixed
CVE-2018-3620	L1TF: L1 terminal fault	No fixes available	Fixed for CSR1/CSR2 only	Fixed
CVE-2018-3639	SSB: Speculative Store Bypass (Spectre, V4)	No fixes available	Fixed for CSR1/CSR2 only	Fixed
CVE-2018-3640	RSRE: Rogue System Register Read (Spectre, V3a)	Fixed for CSR1/CSR2 only	Fixed for CSR1/CSR2 only	Fixed
CVE-2018-3665	Lazy FP: Lazy FPU state restore	No fixes expected[4]	No fixes expected[4]	Fixed
CVE-2018-3693	BCBS: Bounds Check Bypass Store (Spectre, V1.1)	No fixes available	No fixes available	Fixed
CVE-2019-11091	MDSUM: Microarchitectural Data Sampling Uncacheable Memory (Zombieload)	No fixes expected[4]	No fixes expected[4]	Fixed
CVE-2018-12126	MSBDS: Microarchitectural Store Buffer Data Sampling (Fallout)	No fixes expected[4]	No fixes expected[4]	Fixed
CVE-2018-12127	MLPDS: Microarchitectural Load Port Data Sampling	No fixes expected[4]	No fixes expected[4]	Fixed
CVE-2018-12130	MFBDS: Microarchitectural Fill Buffer Data Sampling	No fixes expected[4]	No fixes expected[4]	Fixed

Note:

1. CPDC servers are not affected by the noted CVEs or the impact is minimal.

2. The impact is unknown in case of CPPM / CPMG because these platforms use legacy CPUs, which are not currently supported by the vendor. It is anyway recommended to apply advised fixes to minimize related risks.

3. No fixes are expected for CVE-2017-5754 in case of 32-bit Red Hat Enterprise Linux 5 because of related risks. Please check the following page for more info. https://access.redhat.com/security/cve/cve-2017-5754

4. No fixes are expected because of the current life stage of Red Hat Enterprise Linux 5.

© 2019 Avaya Inc. All Rights Reserved.

Appropriate patches and updates are listed in the following table.

Platform	Kernel SU	Microcode update[1]
CPPM with CS1000 Linux Base	kernel-2.6.18-437.el5.i686.000	-
CPMG, CPDC, COTS or Common Server R1/R2 with CS1000 Linux Base	kernel-PAE-2.6.18-437.el5.i686.000	MPLR33955
CPDC, COTS or Common Server R1/R2 with amsx64 load	kernel-2.6.18-437.el5.x86_64.000	MPLR33955
Any CS1000 CSR3 platform	kernel-2.6.32-754.17.1.el6.i686.000	MPLR33955
Common Server R3 with amsx64 load	kernel-2.6.32-754.17.1.el6.i686.000	MPLR33955

Note:
1. Microcode updates cover Common Servers only.
2. All noted fixes are delivered along with CS1000 R7.6 Service Pack 11.

Performance impact

Traffic testing of the fixes did not show performance degradation that could affect call processing.

Please anyway ensure that the used configuration meets the standard requirements covered in NN43041-200 CS1000 Communication Server 1000E Planning and Engineering.

https://downloads.avaya.com/css/P8/documents/100170484

Workaround or alternative remediation

n/a

Remarks

n/a

© 2019 Avaya Inc. All Rights Reserved.

Patch Notes

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

Backup before applying the patch
n/a
Download
Appropriate patches can be found on the Avaya ESPL Web site https://espl.avaya.com/espl/
Patch install instructions — **Service-interrupting?**
Please check NN43001-407 CS1000 Patching Fundamentals for more info on the patching process. — Yes https://downloads.avaya.com/css/P8/documents/100170376
Verification
n/a
Failure
n/a
Patch uninstall instructions
Please check NN43001-407 CS1000 Patching Fundamentals for more info on the patching process. https://downloads.avaya.com/css/P8/documents/100170376

Security Notes

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

Security risks
n/a
Avaya Security Vulnerability Classification
Medium
Mitigation
Ongoing system changes and maintenance should be done locally using accepted security processes for access and administration.

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.

© 2019 Avaya Inc. All Rights Reserved.