Product Support Notice

PSN #	PSN006040u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 13-Apr-22. This is issue #02, published date: 28-Apr-22.	Severity/risk level	High	Urgency	Immediately

Name of problem	PSN006040u – CMS Spring Cloud Function & Spring4Shell vulnerabilities

Products affected

CMS 19.2.0.3

Problem description

Avaya is aware of the recently identified Spring Cloud Function and Spring4Shell (Spring Core Framework) vulnerabilities (CVE-2022-22963, CVE-2022-22965) and is conducting impact assessments across its portfolio, identifying opportunities for temporary mitigations, if possible, and developing plans for remediation, as appropriate. Reference the *Avaya Product Security* – ***Spring4Shell and Spring Cloud Function Vulnerabilities*** on support.avaya.com for updates.

CMS has recently identified CVE-2022-xxxx and has added assessment below.

CMS 19.2.0.3 is impacted by the Spring4Shell vulnerability.

CMS 19.0.x, CMS 19.1.x and CMS 19.2.x (other than 19.2.0.3) are running Spring4Shell but are not susceptible because they are running Java 8.

Please only follow documented procedures described in this PSN to resolve this issue.

This PSN will be updated as more information is available.

Ensure that you are signed up for Avaya E-notifications so that you will be notified when new issues of this PSN are posted.

Resolution

The resolution for this vulnerability has been identified and a patch is now available.

19.2.0.3 Patch 2 is available for download from PLDS at the following location:

- 19.2.0.3 Patch 2 Download

CMS Patch Installation Instructions:

1. Download cmsweb-R19.2.0.3.ge.m.bin to / on the CMS system.

   Checksum is: 668a93cec6f6ff5a4b2467a7dbdcb6a0

2. Verify the md5 checksum for the downloaded file. Execute the following:

   Prompt> cd /

   Prompt> md5sum cmsweb-R19.2.0.3.ge.m.bin

   Compare the output of this command to the above noted checksum.

   If the numbers do not match, there was a problem with the download, try download again.

3. chmod on the downloaded files to make executable

   Prompt> chmod 744 cmsweb-R19.2.0.3.ge.m.bin

4. Stop the web client

   Prompt> cmsweb stop

5. Install the patch file

   Prompt> ./ cmsweb-R19.2.0.3.ge.m.bin

6. Start the web client

   Prompt> cmsweb start

Workaround or alternative remediation

n/a

Remarks

PSN Revision History
Issue 1 – April 13, 2022: Initial publication.
Issue 2 – April 28, 2022: Updated with fix for vulnerability.

Patch Notes

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

Backup before applying the patch

Always

Download

n/a.

Patch install instructions

n/a

Service-interrupting?

No

Verification

n/a

Failure

n/a

Patch uninstall instructions

n/a

Security Notes

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

Security risks

Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22965
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22963
Reference https://tanzu.vmware.com/security/cve-2022-22963
Reference https://tanzu.vmware.com/security/cve-2022-22965
Reference https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement
Reference https://blog.cloudflare.com/waf-mitigations-spring4shell/
Reference https://spring.io/blog/2022/04/01/spring-framework-rce-mitigation-alternative

Avaya Security Vulnerability Classification

Reference https://support.avaya.com/helpcenter/getGenericDetails?detailId=1399847128146

Mitigation

As noted in this PSN.

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.

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.