Product Support Notice

PSN #	PSN005571u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 19-April-22. This is issue #01, published date 19-April-22.	Severity/risk level	High	Urgency	Immediately	
Name of problem	PSN005571u – Spring Cloud Function & Spring4Shell vulnerabilities for Avaya Aura System Manager, Avaya Aura Standalone WebLM and Solution Deployment Manager Client				

Products affected

Avaya Avaya System Manager – Releases 8.x and 10.1.x

Avaya Aura Standalone WebLM – Releases 8.x and 10.1.x

Solution Deployment Manager (SDM) Client – Releases 8.x and 10.1.x

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.

Internal analysis has determined that Avaya Aura System Manager is not affected by

- CVE-2022-22963: because it is running Java 8 and does not use Apache Tomcat as a servlet container.
  Note: If a scan of System Manager shows this CVE it can be ignored since System Manager is not affected by this CVE for the above-mentioned reasons
- CVE-2022-22965: because it does not use the Spring Cloud function.

Internal analysis has determined that Avaya Aura WebLM is not affected by CVE-2022-22963 and CVE-2022-22965 because it does not use Spring Framework or Spring Cloud function.

Internal analysis has determined that SDM Client is not affected by CVE-2022-22963 and CVE-2022-22965 because it does not use Spring Framework or Spring Cloud function.

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

N/A

Workaround or alternative remediation

N/A

Remarks

PSN Revision History
Issue 1 – April 15, 2022: Initial publication.

Patch Notes

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

N/A

Backup before applying the patch	
Always	
Download	
n/a.	
Patch install instructions	**Service-interrupting?**
n/a	Yes
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.