Product Support Notice

PSN #	PSN006043u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.			
Original publication date: 19-Apr-22. This is issue #01, published date: 19-Apr-22.		Severity/risk level	High	Urgency	Immediately
Name of problem	PSN006043u – Avaya Diagnostic Server and SAL Policy Manager Spring Cloud Function & Spring4Shell vulnerabilities				

Products affected

Avaya Diagnostic Server 3.0, 3.1, 3.2, 3.3, and 4.0.

SAL Policy Manager 3.0, 3.1, 3.2, and 4.0.

BPAR 3.0 (Limited Availability).

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.

Avaya Diagnostic Server 3.0, 3.1, 3.2, 3.3, and 4.0 on all supported platforms including OVA, standalone, etc. running Spring Core Framework are not susceptible to Spring4Shell (CVE-2022-22965).

Internal analysis has determined that SAL Gateway and SLAMon Server of Avaya Diagnostic Server 3.0, 3.1, 3.2, 3.3, and 4.0 releases are not vulnerable to the associated vulnerability CVE-2022-22965 because they are running on Java 8 only. Java 9 and higher is not supported.

Avaya Diagnostic Server 3.0, 3.1, 3.2, 3.3, and 4.0 on all supported platforms including OVA, standalone, etc. do not include Spring Cloud Function and are not susceptible to CVE-2022-22963.

SAL Policy Manager 3.0, 3.1, 3.2, and 4.0 on all supported platforms including OVA, standalone, etc. running Spring Core Framework are not susceptible to Spring4Shell (CVE-2022-22965).

Internal analysis has determined that SAL Policy Manager 3.0, 3.1, 3.2, and 4.0 releases are not vulnerable to the associated vulnerability CVE-2022-22965 because they are running on Java 8 only. Java 9 and higher is not supported.

SAL Policy Manager 3.0, 3.1, 3.2, and 4.0 on all supported platforms including OVA, standalone, etc. do not include Spring Cloud Function and are not susceptible to CVE-2022-22963.

BPAR 3.0 (Limited Availability) running Spring Core Framework is not susceptible to Spring4Shell (CVE-2022-22965).

Internal analysis has determined that BPAR 3.0 (Limited Availability) release is not vulnerable to the associated vulnerability CVE-2022-22965 because it is running on Java 8 only. Java 9 and higher is not supported.

BPAR 3.0 (Limited Availability) does not include Spring Cloud Function and is not susceptible to CVE-2022-22963.

Resolution

NA

Workaround or alternative remediation

NA

Remarks

PSN Revision History

Issue 1 – April 19, 2022: Initial publication.

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	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.

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.