Product Support Notice

PSN #	PSN006042u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 14-Apr-22. This is issue #01, published date: 14-Apr-22.	Severity/risk level	High	Urgency	Immediately

Name of problem	PSN006042u – Proactive Outreach Manager (POM) Spring Cloud Function & Spring4Shell vulnerabilities

Products affected

Proactive Outreach Manager (POM) releases 3.1.3.x, 4.0.x, 4.0.1.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.

Proactive Outreach Manager (POM) has recently identified CVE-2022-22963 and CVE-2022-22965 and has added assessment below.

Proactive Outreach Manager (POM) releases 3.1.3.x, 4.0.x, 4.0.1.x running Spring4Shell are not susceptible.

The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, it is not vulnerable to the exploit. All POM spring boot applications are build using OpenJDK8 and do not use Spring Cloud Function & are deployed as Spring Boot executable jar and are therefore not vulnerable to the exploit.

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

Not Applicable

Workaround or alternative remediation

Not Applicable

Remarks

PSN Revision History
Issue 1 – April 14, 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

n/a

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.