Product Support Notice

PSN #	PSN005963u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.		
Original publication date: 15-Dec-21. This is issue #04, published date: 24-Jan-2022.	Severity/risk level	High	Urgency	Immediately
Name of problem	PSN005963u – Avaya Oceana™ Workspaces Log4j vulnerabilities			

Products affected

Avaya Oceana™ Workspaces, all releases.

Problem description

Avaya is aware of the recently identified Apache Log4j vulnerabilities (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832, CVE-2021-4104) and is conducting impact assessments across its portfolio, identifying opportunities for temporary mitigations, if possible, and developing plans for remediation. Reference the *Avaya Product Security - **Apache Log4j Vulnerability - Impact for Avaya products*** on support.avaya.com for updates

Avaya Oceana™ Workspaces deployed on Avaya Breeze™ and using the log4j provided by it.

Avaya Oceana™ Workspaces Releases 3.2, 3.2.1, 3.2.2, 3.3, 3.4, 3.5, 3.6, 3.6.1, 3.7, 3.8 are impacted by the Log4j2 vulnerability (CVE-2021-44228). Avaya Breeze™ is already on End or sale for these releases, so log4j can't be upgraded. To fix this issue, existing customers on these releases need to upgrade Avaya Breeze™ and Avaya Oceana™ Workspaces to release 3.8.1.0 or later versions.

Avaya Oceana™ Workspaces Releases 3.8.1.0, 3.8.1.1 are also impacted by the Log4j2 vulnerability (CVE-2021-44228). To fix this issue, need to apply patch from Avaya Breeze™ for Log4j2 vulnerability mentioned in PSN https://download.avaya.com/css/public/documents/101079448.

Avaya Oceana™ Workspaces has been assessed against the Apache Log4J (CVE-2021-45046) vulnerability and it has been determined that it is not vulnerable to this issue.

Avaya Oceana™ Workspaces has been assessed against the Apache Log4J (CVS-2021-45105) vulnerability and it has been determined that it is not vulnerable to this issue.

Avaya Oceana™ Workspaces has been assessed against the Apache Log4J (CVE-2021-44832) vulnerability and it has been determined that it is not vulnerable to this issue.

Avaya Oceana™ Workspaces has been assessed against the Apache Log4J (CVE-2021-4104) vulnerability and it has been determined that it is not vulnerable to this issue.

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

1. Need to upgrade Avaya Breeze™ and Avaya Oceana™ Workspaces to release 3.8.1.0 or later versions.
2. Apply Log4j2 vulnerability patches from Breeze. Information available on PSN https://download.avaya.com/css/public/documents/101079448

Workaround or alternative remediation

NA

Remarks

Issue 1 – December 15, 2021: Initial publication.
Issue 2 – December 21, 2021: Updated to include assessment for CVE-2021-45046, CVE-2021-45105
Issue 3 – January 7, 2022: Updated to include assessment for CVE-2021-44832, CVE-2021-4104
Issue 4 – January 24, 2022: Updated to reflect versions with supported Breeze patches.

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-2021-44228
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45105
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44832
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4104

Reference https://logging.apache.org/log4j/2.x/security.html

Avaya Security Vulnerability Classification

Reference www.avaya.com/emergencyupdate

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.