Product Support Notice

PSN #	PSN005946u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.			
Original publication date 17-Dec-2021 This is Issue #07, published date: 04-Feb-2022.		Severity/risk level	High	Urgency	Immediately
Name of problem	PSN005946u – IP Office Log4j2 vulnerability (CVE-2021-44228)				

Products affected

IP Office Perpetual, Subscription, Server Edition, Powered By VM

Releases: 11.0.4.1 to 11.0.4.6. 11.1.0.0 to 11.1.2.0

Powered by Avaya IP Office™ (FP) Releases: 3.0.3, 3.0.4

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, CVE-2022-23302, CVE-2022-23305, CVE-2022-23307) 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.

The IP Office applications: one-X Portal (Windows and Linux), Media Manager, WebRTC Gateway and Web Collaboration are impacted by the Log4j vulnerability CVE-2021-44228 only.

This issue does not affect IP Office Basic Edition, Essential Edition, Branch deployments or IP Office Powered By Containers. Preferred Edition without any of the vulnerable applications active is also not affected.

Please only follow documented procedures described in this PSN to resolve this issue.
This PSN will be updated as more information is available.

Resolution

IP Office Critical Patches (CP) are now available for both 11.0.4 SP6 and 11.1.2 on the respective support.avaya.com software pages (links below). These apply to all IP Office platforms including UCMV1/V2.
In addition, IP Office Service Pack releases 11.0.4 SP7 and 11.1.2 SP1 are now available that include the Critical Patch and no other changes.

11.0.4: https://support.avaya.com/downloads/download-details.action?contentId=1399821931920&productId=P0160&releaseId=11.0.x
11.1.2: https://support.avaya.com/downloads/download-details.action?contentId=1399835691661&productId=P0160&releaseId=11.1.x

Workaround or alternative remediation

Ensure one-X Portal for IP Office, Media Manager, WebRTC Gateway and Web Collaboration services are disabled

Remarks

Issue 1 – December 15, 2021: Initial publication.
Issue 2 – December 16, 2021: Clarification of unaffected components.
Issue 3 – December 16, 2021: Further clarification of unaffected components.
Issue 4 – December 17, 2021: Update of resolution and problem description
Issue 5 – December 20, 2021: Update of resolution to include UCMV1/V2
Issue 6 – January 5, 2022: Inclusion of CVE-2021-4104 and CVE-2021-2021-44832
Issue 7 – February 4, 2022: Inclusion of CVE-2022-23302, CVE-2022-23305, CVE-2022-23307, plus 11.0.4 SP7 and 11.1.2 SP1

Patch Notes

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

- Please refer to any patch release notes contained with the patch

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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23302
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23305
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23307

Reference https://logging.apache.org/log4j/2.x/security.html
Reference https://logging.apache.org/log4j/1.2/

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.