Product Support Notice

PSN #	PSN005948u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.			
Original publication date: 15-Dec-21. This is issue #05, published date: 1-Feb-22.		Severity/risk level	High	Urgency	Immediately
Name of problem	PSN005948u – Intelligent Customer Routing (ICR) Log4j vulnerabilities.				

Products affected

Intelligent Customer Routing (ICR) release 7, 7.0.1, 7.0.2 and 8.0.

Problem description

Avaya is aware of the recently identified Apache Log4j vulnerability (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

All Intelligent Customer Routing (ICR) releases are running Log4jv1 that are not susceptible.

Internal analysis has determined that ICR releases are not vulnerable to the associated below mentioned vulnerabilities –

- CVE-2021-4104 (Log4j 1.x JMSAppender). Although Log4j 1.x is used in the software it is not vulnerable because JMSAppender is not used in any of the log4j configurations for ICR by default.
- CVE-2022-23302 (Log4j 1.x JMSSink). Although Log4j 1.x is used in the software it is not vulnerable because JMSSink is not used in any of the log4j configurations for ICR by default.
- CVE-2022-23305 (Log4j 1.x JDBCAppender). Although Log4j 1.x is used in the software it is not vulnerable because JDBCAppender is not used in any of the log4j configurations for ICR by default.
- CVE-2022-23307 (Log4j 1.x Chainsaw). Although Log4j 1.x is used in the software it is not vulnerable because Chainsaw is not used in any of the log4j configurations for ICR by default.

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

Refer to the Workaround/alternative remediation section below.

Workaround or alternative remediation

For log4j 1.x, JMSAppender, JMSSink, JDBCAppender and Chainsaw should not be configured. If it is configured – remove it from Log4j configuration file and restart the appropriate ICR component.

Remarks

Issue 1 – December 15, 2021: Initial publication.
Issue 2 – December 20, 2021: CVE-2021-45046
Issue 3 – December 21, 2021: CVE-2021-45105
Issue 4 – January 05, 2022: CVE-2021-44832, CVE-2021-4104
Issue 5 – February 1, 2022: CVE-2022-23302, CVE-2022-23305, CVE-2022-23307

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://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.