Product Support Notice

PSN #	PSN005971u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.	

Original publication date: 31-Jan-2022. This is issue #04, published date: 31-Jan-2022.	Severity/risk level	High	Urgency	Immediately

Name of problem	Desktop Collector Snap-in Log4j2 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)

Products affected

Desktop Collector Snap-in, 3.3

Desktop Collector Snap-in, 3.3.x

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

Internal analysis has determined that Desktop Collector Snap-in releases are not vulnerable to the associated vulnerability CVE-2022-23302 (Log4j 1.x JMSSink) although Log4j 1.x is used in the software. This is because JMSSink is not used or configured in any of the log4j configurations for Desktop Collector Snap-in by default.

Internal analysis has determined that Desktop Collector Snap-in releases are not vulnerable to the associated vulnerability CVE-2022-23305 (Log4j 1.x JDBCAppender) although Log4j 1.x is used in the software. This is because JDBCAppender is not used or configured in any of the log4j configurations for Desktop Collector Snap-in by default.

Internal analysis has determined that Desktop Collector Snap-in releases are not vulnerable to the associated vulnerability CVE-2022-23307 (Log4j 1.x Chainsaw) although Log4j 1.x is used in the software. This is because Chainsaw is not used or configured in any of the log4j configurations for Desktop Collector Snap-in 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

Not Impacted

Workaround or alternative remediation

NA

Remarks

PSN Revision History

PSN Revision History

Issue 1 – December 17, 2021: Initial publication.

Issue 2 – December 21, 2021: Updated and published the same document with Version 4 PSN template.

Issue 3 – January 07, 2022: Updated and published the same document with Version 5 PSN template.

Issue 3 – January 31, 2022: Updated and published the same document with Version 6 PSN template.

Patch Notes

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

Backup before applying the patch
Always

Download
NA

Patch install instructions	Service-interrupting?
NA	Yes

Verification
NA

Failure
NA

Patch uninstall instructions
NA

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.