Product Support Notice

PSN #	PSN020554u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.			
Original publication date: 14-Dec-21. This is Issue #07, published date: 04-Feb-22.		Severity/risk level	High	Urgency	Immediately
Name of problem	PSN020554u - Avaya Session Border Controller for Enterprise (ASBCE) Log4j2 vulnerabilities				

Products affected

Avaya Session Border Controller for Enterprise (ASBCE), 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.

The table below outlines which releases of ASBCE are impacted by the vulnerabilities. Details for fixes are in the Resolution section of this PSN.

ASBCE Release →	**8.0.1 through 8.1.3**	**8.0.0, 7.x and earlier**
Impacted by CVE-2021-44228	yes	no
Impacted by CVE-2021-45046	yes	no
Impacted by CVE-2021-45105	yes	no
Impacted by CVE-2021-44832	yes	no
Impacted by CVE-2021-4104	no	no

Important Notes:

1. ASBCE versions 8.0.0, 7.x and earlier do not utilize Log4j 2.x and therefore are not impacted by the by the Log4j 2.x vulnerabilities (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832).

2. ASBCE versions 8.x (8.0.1, 8.1.0, 8.1.1, 8.1.2, 8.1.3) are vulnerable to the Log4j 2.x exploits. Avaya has released hotfixes to address all CVEs. Reference the resolution section of this PSN for details on the current hotfixes.

3. Internal analysis has determined that ASBCE releases are not vulnerable to the associated vulnerability CVE-2021-4104 (Log4j 1.x JMSAppender) although Log4j 1.x is used in software. This is because JMSAppender is not used in any of the log4j configurations.

4. Internal analysis has determined that ASBCE releases 8.0.0, 7.x and earlier are not vulnerable to the associated vulnerability CVE-2021-44832 as those releases do not utilize Log4j 2.x and the use of Log4j 1.x does not utilize the JDBCAppender in any of the Log4j configurations and there is no direct way to modify the Log4j configuration.

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

ASBCE 8.0.0, 7.x and earlier are not impacted by any of these vulnerabilities, hence no action needed on ASBCE version 8.0.0, 7.x or earlier.

Hotfixes listed below address the impacted CVEs listed in the table above. These hotfixes can directly be applied on top of older versions of Log4j hotfixes (mentioned in previous issues of this PSN), if those older versions of hotfix have been applied before. Otherwise, just apply the latest hotfixes listed below.

Important: ASBCE versions 8.0.1 will need to upgrade to 8.1.2 or 8.1.3 with the latest hotfix and then apply the specific log4j hotfix mentioned below to mitigate the problem. ASBCE version 8.1.0 and 8.1.1 have hotfixes (below) for log4j except CVE-2021-44832. These two branches need to move up to 8.1.2 or 8.1.3 or 10.1 to mitigate that CVE.

The following hotfixes address all vulnerabilities listed in the table above with the exception of CVE-2021-44832 in 8.1.0 and 8.1.1 branches.

For ASBCE version 8.1.0

Install the hotfix **sbce-8.1.0.0-14-21464-hotfix-12212021-log4jFix.tar.gz** to address the vulnerabilities. (except CVE-2021-44832. For fixing this CVE, user need to upgrade to 8.1.2 or 8.1.3 or 10.1)

For ASBCE version 8.1.1

Install the hotfix **sbce-8.1.1.0-26-21464-hotfix-12212021-log4jFix.tar.gz** to address the vulnerabilities. (except CVE-2021-44832. For fixing this CVE, user need to upgrade to 8.1.2 or 8.1.3 or 10.1)

For ASBCE version 8.1.2

Install the hotfix **sbce-8.1.2.0-37-21486-hotfix-01062022.tar.gz** (i.e. 8.1.2.0Hotfix-8) to address all log4j vulnerabilities (include CVE-2021-44832).

For ASBCE version 8.1.3

Install the hotfix **sbce-8.1.3.0-38-21537-hotfix-02042022-log4jFix.tar.gz** to address all log4j vulnerabilities (include CVE-2021-44832).

Details on PLDS download IDs and installation instructions for the above four hotfixes are located in the **Patch Notes** section of this PSN.

Workaround or alternative remediation

While Avaya recommends following the steps in the Resolution section of this PSN, as an alternative to the hotfixes identified in the Resolution section of this PSN, the steps outlined below can also be applied to ASBCE version 8.1.2/8.1.3 to mitigate the issue.

For ASBCE version 8.1.2

Make sure hotfix-5 (i.e. sbce-8.1.2.0-37-21246-hotfix-09282021.tar.gz) or higher is installed on the system.

For ASBCE version 8.1.3

Make sure hotfix-1 (i.e. sbce-8.1.3.0-38-21245-hotfix-09242021.tar.gz) or higher is installed on the system.

1. Login to the CLI as root.
2. Make a copy of the following file as a backup:

   ```
   cp /usr/local/ipcs/etc/sys.profile  /tmp/sys.profile.ORIG
   ```

3. Add the following two lines to the end of /usr/local/ipcs/etc/sys.profile :

   ```
   TOMCAT_JVM_OPTS=-Dlog4j2.formatMsgNoLookups=true
   TOMCAT_JVM_8_OPTS=-Dlog4j2.formatMsgNoLookups=true
   ```

4. Save the file.

5. Restart Tomcat with the following commands:

   ```
   service ipcs-ems stop
   service ipcs-ems start
   ```

6. If a problem occurs, recover the original sys.profile file
   a. cp /tmp/sys.profile.ORIG   /usr/local/ipcs/etc/sys.profile
   b. Restart Tomcat with the following commands:

```
service ipcs-ems stop
service ipcs-ems start.
```

This should be performed on ALL DEVICES – EMS AND SBCE.

Remarks

PSN Revision History:
Issue 1 – December 14, 2021: Initial publication
Issue 2 – December 15, 2021: NEW hotfixes in 8.1.2 and 8.1.3 to address BOTH CVE-2021-44228 and CVE-2021-45046.
Issue 3 – December 16, 2021: Correction – 8.0.0 is not susceptible. Added instructions to install patch on EMS first.
Issue 4 – December 16, 2021 : NEW hotfixes in 8.1.0 and 8.1.1 to address BOTH CVE-2021-44228 and CVE-2021-45046.
Issue 5 – December 21, 2021: NEW hotfixes in 8.1.0, 8.1.1, 8.1.2, 8.1.3 to address CVE-2021-44228, CVE-2021-45046 and CVE-2021-45105)
Issue 6 – January 07, 2022: Updated to include information for CVE-2021-44832 and CVE-2021-4104.
Issue 7 – February 04, 2022: NEW hotfixes for CVE-44832 in 8.1.2 and 8.1.3.

Patch Notes

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

Backup before applying the patch
Take a backup of ASBCE and save it on an external storage

Download

Download the patch from https://plds.avaya.com

ASBCE version 8.1.0.0
PLDS Download ID: SBCE0000285
Patch Name: sbce-8.1.0.0-14-21464-hotfix-12212021-log4jFix.tar.gz
Md5sum: 60cd35f469c498249b298e5f638ecb28

ASBCE version 8.1.1.0
PLDS Download ID: SBCE0000286
Patch Name: sbce-8.1.1.0-26-21464-hotfix-12212021-log4jFix.tar.gz
Md5sum: 21f7a92bd66aaa6bb80209d4f36c40b8

ASBCE version 8.1.2.0
PLDS Download ID: SBCE0000290
Patch Name: sbce-8.1.2.0-37-21486-hotfix-01062022.tar.gz
Md5sum: 6672536dc89bf671ae4ff58be92c13b0
(*replaces previous SBCE0000287; sbce-8.1.2.0-37-21460-hotfix-12202021-log4jFix.tar.gz)*

ASBCE version 8.1.3.0
PLDS Download ID: SBCE0000291
Patch Name: sbce-8.1.3.0-38-21537-hotfix-02042022-log4jFix.tar.gz
Md5sum: e839f93c3c9347d00ba9ba3392b2f05c
(replaces previous SBCE0000288; sbce-8.1.3.0-38-21460-hotfix-12202021-log4jFix.tar.gz)

Patch install instructions	Service-interrupting? Yes

Important: Install the patch during a maintenance window to avoid service disruption.
Install the patch over the SBCE and EMS (version: 8.1.0.0, 8.1.1.0, 8.1.2.0 or 8.1.3.0)

Note: For HA SBCE, install the patch on EMS first, then install the patch on the secondary SBCE and perform failover. Later, install the patch on new Secondary SBCE.

For ASBCE version 8.1.0

Install the hotfix **sbce-8.1.0.0-14-21464-hotfix-12212021-log4jFix.tar.gz** to address the vulnerabilities (except CVE-2021-44832. For fixing this CVE, user need to upgrade to 8.1.2 or 8.1.3 or 10.1).

For ASBCE version 8.1.1

Install the hotfix **sbce-8.1.1.0-26-21464-hotfix-12212021-log4jFix.tar.gz** to address the vulnerabilities (except CVE-2021-44832. For fixing this CVE, user need to upgrade to 8.1.2 or 8.1.3 or 10.1).

For ASBCE version 8.1.2

Install the hotfix **sbce-8.1.2.0-37-21486-hotfix-01062022.tar.gz** to address the vulnerabilities.

For ASBCE version 8.1.3

Install the hotfix **sbce-8.1.3.0-38-21537-hotfix-02042022-log4jFix.tar.gz** to address the vulnerabilities.

Install instructions:

Stop the application using command "/etc/init.d/ipcs-init stop" and please wait for all the process to be stopped.

Note: Following is the install procedure for 8.1.3 patch. 8.1.2, 8.1.1 and 8.1.0 patch installation procedure is similar, just replace the file/directory name accordingly.

1. Copy the tar file "sbce-8.1.3.0-38-21537-hotfix-02042022-log4jFix.tar.gz" to /home/ipcs directory.
2. Login to the CLI of SBCE as user ipcs.
3. Switch user to root with the command: su - root
4. Change directory to /home/ipcs with the command: cd /home/ipcs
5. Verify md5sum of the patch file matches with the md5sum on PLDS i.e. e839f93c3c9347d00ba9ba3392b2f05c

   Command: md5sum sbce-8.1.3.0-38-21537-hotfix-02042022-log4jFix.tar.gz
6. Untar the patch tar file

   #tar -zxvf sbce-8.1.3.0-38-21537-hotfix-02042022-log4jFix.tar.gz
7. Go to directory sbce-8.1.3.0-38-21537-hotfix-02042022-log4jFix

   #cd sbce-8.1.3.0-38-21537-hotfix-02042022-log4jFix
8. To apply the patch , run below command

   #sh install_hotfix.sh
9. After applying the patch, system must be rebooted.

   # reboot

Verification instruction:

1. rpm -qa | grep tomcat and make sure it is apache-tomcat-minimal-9.0.56-4.noarch in 8.1.3 and 8.1.2.

   or

2. cd /usr/local/tomcat/log4j2/lib/

   ls -lrt

   and check if log4j version is 2.17.1 (in 8.1.2 and 8.1.3. 2.17.0 in 8.1.1 and 8.1.0).

Verification

Patch activation instructions include verification instructions.

Failure

Contact Technical Support.

Patch uninstall instructions

Note: For HA SBCE's, uninstall the patch first on secondary SBCE, and perform failover. Later, uninstall the patch on the new Secondary SBCE.

Important: Make sure to uninstall the patch during a maintenance window to avoid service disruption.

1. Login to the CLI of SBCE's as user ipcs.
2. Switch user to root:
   ```
   su – root
   ```
3. Go to directory sbce-8.1.3.0-38-21537-hotfix-02042022-log4jFix
   ```
   #cd sbce-8.1.3.0-38-21537-hotfix-02042022-log4jFix
   ```
4. 4. To remove the patch, run below command
   ```
   #sh remove_hotfix.sh
   ```
5. After removing the patch, system must be rebooted.
   ```
   # reboot
   ```

Note: patch uninstall will rollback the RPM's to GA version. You must re-install any other patch, if installed previously.

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.