Product Support Notice

PSN #	PSN006051u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 11-May-22. This is Issue #01, published date: 11-May-22.	Severity/risk level	High	Urgency	Immediately

Name of problem	Avaya Session Border Controller for Enterprise (ASBCE) Spring4Shell and Spring Cloud Function Vulnerabilities

Products affected

Avaya Session Border Controller for Enterprise (ASBCE), 8.0.1, 8.1.0, 8.1.1, 8.1.2, 8.1.3, 8.1.3.1, 10.1

Problem description

Avaya is aware of the recently identified Spring4Shell and Spring Cloud Function Vulnerabilities (CVE-2022-22965 [Spring Project/VMware Security Alert], CVE-2022-22963 [Spring Project/VMware Security Alert]) 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 - Spring4Shell and Spring Cloud Function Vulnerabilities* 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 10.1.0**	**8.0.0, 7.x and earlier**
Impacted by CVE-2022-22965	yes	no
Impacted by CVE-2022-22963	yes	no

Important Notes:

1. ASBCE versions 8.0.0, 7.x and earlier do not utilize spring VMC and therefore are not impacted by the Spring4Shell and Spring Cloud Function Vulnerabilities.

2. ASBCE versions 8.0.1, 8.1.0, 8.1.1, 8.1.2, 8.1.3, 8.1.3.1 and 10.1 are vulnerable to the Spring4Shell and Spring Cloud Function Vulnerabilities. Avaya has released hotfixes to address above CVEs. Reference the resolution section of this PSN for details on the current hotfixes.

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.

Important: ASBCE versions 8.0.1, 8.1.0, 8.1.1, 8.1.2, and 8.1.3 will need to upgrade to 8.1.3.1 (i.e. 8.1.3SP1) or above and then apply the hotfix mentioned below to mitigate the problem.

The following hotfixes address all vulnerabilities listed in the table above.

For ASBCE version 8.1.3.1

Install the 8.1.3.1 hotfix-1 **sbce-8.1.3.1-39-21939-hotfix-05042022.tar.gz** to address the vulnerabilities.

For ASBCE version 10.1

Install the 10.1 hotfix **sbce-10.1.0.0-xx-xxxxx-hotfix-xxxxxxxx.tar.gz (will be released around May 15, 2022)** to address the vulnerabilities.

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

N.A.

Remarks

PSN Revision History:
Issue 1 – May 11, 2022: Initial publication

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 8.1.3.1

PLDS Download ID: SBCE0000307
Patch Name: sbce-8.1.3.1-39-21939-hotfix-05042022.tar.gz
Md5sum: e891568a7bfdc0b0300a2ed3cd389f2e

ASBCE version 10.1.0.0 (will be released around May 15, 2022)

PLDS Download ID: SBCExxxxxxxx
Patch Name: sbce-10.1.0.0-xx-xxxxx-hotfix-xxxxxxxxxx.tar.gz
Md5sum: xxxxxxxxxxxx

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.

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 8.1.3.1

Install the hotfix **sbce-8.1.3.1-39-21939-hotfix-05042022.tar.gz** to address the vulnerabilities

For ASBCE version 10.1.0

Install the hotfix **sbce-10.1.0.0-xx-xxxxx-hotfix-xxxxxxxx-xxxxx.tar.gz (will be released around May 15, 2022)** 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 8.1.3.1 patch. 10.1 patch installation procedure is similar, just replace the file/directory name accordingly.

1. Copy the tar file "sbce-8.1.3.1-39-21939-hotfix-05042022.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. e891568a7bfdc0b0300a2ed3cd389f2e
   Command: md5sum sbce-8.1.3.1-39-21939-hotfix-05042022.tar.gz
6. Untar the patch tar file
   #tar -zxvf sbce-8.1.3.1-39-21939-hotfix-05042022.tar.gz
7. Go to directory sbce-8.1.3.1-39-21939-hotfix-05042022
   #cd sbce-8.1.3.1-39-21939-hotfix-05042022
8. To apply the patch , run below command
   #sh install_hotfix.sh
9. After applying the patch, system must be rebooted.
   # reboot

Verfication

Verification instruction:

User can verify with the following CLI command:

```
find / -name spring-webmvc-*.jar
```

This will show a list of Spring MVC JAR files, which should show the following if the patch is applied:

```
[root@SBC ~]# find / -name spring-webmvc-*.jar
/usr/local/ipcs/web/cli/lib/spring-webmvc-5.3.19.jar
/usr/local/ipcs/web/gui/WEB-INF/lib/spring-webmvc-5.3.19.jar
/usr/local/ipcs/web/api/WEB-INF/lib/spring-webmvc-5.3.19.jar
```

If the Spring MVC version is 5.3.19 or above, then the patch is applied. Also note, this patch should be applied to every device, EMS, SBCE, or SingleBox.

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-8.1.3.1-39-21939-hotfix-05042022
   #cd sbce-8.1.3.1-39-21939-hotfix-05042022
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-2022-22965

Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22963

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

Avaya Security Vulnerability Classification

Reference Avaya Support

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.