Product Support Notice

PSN #	PSN005949u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 15-Dec-21. This is Issue #12, published date: 9-Mar-22.	Severity/risk level	High	Urgency	Immediately

Name of problem	PSN005949u - Avaya Breeze™ Platform Log4j vulnerabilities

Products affected

Avaya Breeze®, Releases 3.6.x, 3.7.x, 3.8.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) 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.

Avaya Breeze™ Platform, 3.6.x, 3.7.x and 3.8.x, are impacted by the Log4j 2.x vulnerability (CVE-2021-44228).

Avaya Breeze™ Platform, 3.6.x, 3.7.x and 3.8.x are protected using following mechanisms:

1. Avaya Breeze™ Platform can only by accessed by authenticated users.
2. Avaya Breeze™ Platform access is governed by rule-based authorization. Authenticated users can only use platform functionalities which are allowed as per the assigned user role.

With above protection mechanisms, it's very hard to exploit the Avaya Breeze™ Platform using the CVE-2021-44228 vulnerability.

Avaya snap-ins are not vulnerable unless they have published a specific PSN.

Resolution

To provide greater security, Log4j 2.x libraries in the Avaya Breeze™ Platform will be updated through a software patch as follows:

- Avaya Breeze® patch **ce-patch-3.6.0.3.01360308.bin** (PLDS ID = **AB000000282**) applies to Avaya Breeze® 3.6.0.3 GA software (3.6.0.3.360308) and includes the Log4j version 2.16.0 that addresses the CVE-2021-44228 vulnerability and the CVE-2021-45046 vulnerability.
- Avaya Breeze® patch **ce-patch-3.7.0.0.09370008.bin** (PLDS ID = **AB000000283**) applies to Avaya Breeze® 3.7.0.0 GA software (Breeze-3.7.0.0.370008) and includes Log4j version 2.16.0 that addresses the CVE-2021-44228 vulnerability and the CVE-2021-45046 vulnerability.
- Avaya Breeze® patch **ce-patch-3.7.0.2.01370202.bin** (PLDS ID = **AB000000279**) applies to Avaya Breeze® 3.7.0.2 GA software (3.7.0.2.370202) and includes the Log4j version 2.15.0 that addresses the CVE-2021-44228 vulnerability.
- Avaya Breeze® patch **ce-patch-3.8.0.0.01380018.bin** (PLDS ID = **AB000000284**) applies to Avaya Breeze® 3.8.0.0 GA software (3.8.0.0.380018) and includes the Log4j version 2.17.0 that addresses the CVE-2021-44228 vulnerability.
- Avaya Breeze® patch **ce-patch-3.8.0.2.01380204.bin** (PLDS ID = **AB000000280**) applies to Avaya Breeze® 3.8.0.2 GA software (3.8.0.2.380204) and includes the Log4j version 2.15.0 that addresses the CVE-2021-44228 vulnerability.
- Avaya Breeze® patch **ce-patch-3.8.1.0.08381005.bin** (PLDS ID = **AB000000281**) applies to Avaya Breeze® 3.8.1.0 GA software (3.8.1.0.381005) and includes the Log4j version 2.15.0 that addresses the CVE-2021-44228 vulnerability.

The aforementioned patches will address the Apache Log4j vulnerability (CVE-2021-44228).
Breeze has been assessed against the Apache Log4j (CVE-2021-45046) vulnerability and it has been determined that Breeze is not vulnerable to this issue.

Breeze has been assessed against the Apache Log4j (CVS-2021-45105) vulnerability and it has been determined that Breeze is not vulnerable to this issue.

Breeze has been assessed against the Apache Log4j (CVE-2021-44832) vulnerability and it has been determined that Breeze is not vulnerable to this issue.

Breeze has been assessed against the Apache Log4j (CVE-2021-4104) vulnerability and it has been determined that Breeze is not vulnerable to this issue.

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

Workaround or alternative remediation

n/a

Remarks

Issue 1 – December 15, 2021: Bug fixes for Log4j security vulnerability as described in the aforementioned *Resolution* section are made available.

Issue 2 – December 16, 2021: Clarification and additional information provided in *Resolution* and *Patch Notes* sections.

Issue 3 – December 16, 2021: Updated this *Remarks* section.

Issue 4 – December 16, 2021: Corrected a typo in Patch Notes section where it referenced 3.8.0.1 instead of 3.8.1.0.

Issue 5 – December 17, 2021: Includes information indicating the Breeze is not vulnerable to CVE-2021-45046 as well as patch information for Breeze 3.6.x. and additional Security Notes.

Issue 6 – December 21, 2021: Includes information indicating the Breeze is not vulnerable to CVS-2021-45105 in *Problem Description* and *Resolution* section.

Issue 7 – December 21, 2021: Includes additional information about upgrade paths in section *Patch Notes*.

Issue 8 – December 22, 2021: Updated Products Affected, Problem Description and References to fix typos about Log4j 2.x libraries.

Issue 9 – January 6, 2022: Updated information about CVE-2021-44832, CVE-2021-4104 in *Resolution*, *Security Notes* and *Patch Notes* to clarify upgrades required.

Issue 10 – January 31, 2022: Added patch information for Breeze release 3.8.0.0.

Issue 11 – February 14, 2022: Added patch information for Breeze release 3.7.0.0.

Issue 12 – March 8, 2022: Revised to correct minor typographical errors.

Patch Notes

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

Important: The installation of this patch will require service interruption and therefore an appropriate maintenance window should be secured

Important: This patch cannot be reverted and therefore is it recommended to take a VMware snapshot before proceeding and removing the snapshot within 24 hours after applying this patch

Important: This patch must be installed on top of the applicable Avaya Breeze® software:

- For Avaya Breeze® 3.6.0.3 apply patch **ce-patch-3.6.0.3.01360308.bin** (PLDS ID = **AB000000282**) on top of the Avaya Breeze® 3.6.0.3 GA **Breeze- 3.6.0.3.360308.ova** software only.

  If existing Avaya Breeze® system is on any of the following versions:

  - 3.6.0.0 GA
  - 3.6.0.1 GA
  - 3.6.0.2 GA

  then, it needs to be upgraded to 3.6.0.3 GA before applying the patch **ce-patch-3.6.0.3.01360308.bin.**

- For Avaya Breeze® 3.7.0.0 apply patch **ce-patch-3.7.0.0.09370008.bin** (PLDS ID = **AB000000283**) on top of the Avaya Breeze® 3.7.0.0 GA **Breeze-3.7.0.0.370008.ova** software only.
- For Avaya Breeze® 3.7.0.2 apply patch **ce-patch-3.7.0.2.01370202.bin** (PLDS ID = **AB000000279**) on top of the Avaya Breeze® 3.7.0.2 GA **Breeze-3.7.0.2.370202.ova** software only.

  If existing Avaya Breeze® system is on 3.7.0.1 GA, then, it needs to be upgraded to 3.7.0.2 GA before applying the patch **ce-patch-3.7.0.2.01370202.bin.**

- For Avaya Breeze® 3.8.0.0 apply patch **ce-patch-3.8.0.0.01380018.bin** (PLDS ID = **AB000000284**) on top of the Avaya Breeze® 3.8.0.0 GA **Breeze-3.8.0.0.380018.ova** software only.

- For Avaya Breeze® 3.8.0.2 apply patch **ce-patch-3.8.0.2.01380204.bin** (PLDS ID = **AB000000280**) on top of the Avaya Breeze® 3.8.0.2 GA **Breeze-3.8.0.2.380204.ova** software only.

  If existing Avaya Breeze® system is on any of the following versions:

  - 3.8.0.1 GA

  Then, it needs to be upgraded to 3.8.0.2 GA before applying the patch **ce-patch-3.8.0.2.01380204.bin.**

- For Avaya Breeze® 3.8.1.0 apply patch **ce-patch-3.8.1.0.08381005.bin** (PLDS ID = **AB000000281**) on top of the Avaya Breeze® 3.8.1.0 patch #1 **ce-patch-3.8.1.0.07381005.bin** (PLDS ID = **AB000000278**) software only.

Important: Please place the **cluster** in Deny New Service when applying this patch. Application of the patch can be done simultaneously with other nodes in the cluster. A cluster reboot is required after completing this patch application. Please consult *Deploying Avaya Breeze® Platform* and *Upgrading Avaya Breeze® Platform* for further information.

Backup before applying the patch

Backup data remotely prior to patch installation. Breeze supports ClusterDB backup/restore from the System Manager Breeze EM

Download

The Avaya Breeze® patches **ce-patch-3.7.0.2.01370202.bin, ce-patch-3.8.0.2.01380204.bin** and **ce-patch-3.8.1.0.08381005.bin** files can be downloaded from Avaya Support:

1. Go to Avaya Support and enter your Username and Password, then click LOG IN.
2. Mouse over **Support by Product** at the top of the page and click **Downloads** in the menu.
3. For the 3.7.0.0 patch,
   a. in the **Enter Your Product Here** box, enter “Breeze” and select **Avaya Breeze® Platform** with Product Release **3.7.x** for your installation.
   b. Click **Avaya Breeze® 3.7.0.0 Platform and Patches, 3.7.x**.
4. For the 3.7.0.2 patch,
   a. in the **Enter Your Product Here** box, enter “Breeze” and select **Avaya Breeze® Platform** with Product Release **3.7.x** for your installation.
   b. Click **Avaya Breeze® 3.7.0.2 Platform and Patches, 3.7.x**.
5. For the 3.8.0.0 patch,
   a. in the **Enter Your Product Here** box, enter “Breeze” and select **Avaya Breeze® Platform** with Product Release **3.8.x** for your installation.
   b. Click **Avaya Breeze® 3.8.0.0 Platform and Patches, 3.8.x**.
6. For the 3.8.0.2 patch,
   a. in the **Enter Your Product Here** box, enter “Breeze” and select **Avaya Breeze® Platform** with Product Release **3.8.x** for your installation.
   b. Click **Avaya Breeze® 3.8.0.2 Platform and Patches, 3.8.x**.
7. For the 3.8.1.0 patch,
   a. in the **Enter Your Product Here** box, enter “Breeze” and select **Avaya Breeze® Platform** with Product Release **3.8.x** for your installation.
   b. Click **Avaya Breeze® 3.8.1.0 Platform and Patches, 3.8.x**.
8. Find the correct file and click on it to download.

Or, download directly from PLDS using download ID:

- For 3.7.0.0 use PLDS ID AB000000283
- For 3.7.0.2 use PLDS ID AB000000279
- For 3.8.0.0 use PLDS ID AB000000284

- For 3.8.0.2 use PLDS ID AB000000280
- For 3.8.1.0 use PLDS ID AB000000281

Patch install instructions	Service-interrupting?
Please refer to Upgrading Avaya Breeze® platform (chapter 4) for information about Patching	Yes

Verification

Verify ALL Breeze nodes have been patched and the Breeze dashboard reports all green prior to placing the cluster back into service from the SMGR UI.

Failure

Contact Avaya Technical Support

Patch uninstall instructions

This patch cannot be uninstalled and therefore is it recommended to take a VMware snapshot before proceeding and removing the snapshot within 24 hours after applying this 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://logging.apache.org/log4j/2.x/security.html

Avaya Security Vulnerability Classification

Reference www.avaya.com/emergencyupdate

Mitigation

n/a

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.

Business Partner Notes

Additional information for Business Partners

n/a

Avaya Notes

Additional information for Tier 3, Tier 4, and development

Maestro/Siebel tickets: n/a

MRs: See Resolution section above.