Product Support Notice

© 2026 Avaya LLC. All Rights Reserved.

PSN#	PSN006515u

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

Original publication date: 26-October-2026, This is Issue # 04. published date: 06-November-2026.

Severity/risk level: High | Urgency: Immediately

Name of problem

Avaya Experience Portal CVE-2026-109618 and CVE-2026-109619 (PHP2SHELL Vulnerabilities)

Products affected

Avaya Experience Portal,Versions: 8.0, 8.1.0, 8.1.1, 8.1.2.x

Problem description

Avaya has determined that this product contains PHP code that has the vulnerabilities listed in *CVE-2026-109618* and *CVE-2026-109619*.

The resolution for Avaya Experience Portal 8.1.2.x, 8.1.1, 8.1.0 and 8.0 is available, refer to the **Resolution** section below.
This Resolution is applicable for Avaya Experience Portal Deployments on Avaya RHEL (AVL), and not applicable for Avaya Experience Portal 'Software Only' Solution.

Customers who are on Avaya Experience Portal 7.2.3 and earlier are not impacted with the vulnerability.

If you have any questions on Avaya's remediation activities for these vulnerabilities, please contact Avaya or the appropriate business partner.

CVE References:

- CVE-2026-109618 - https://nvd.nist.gov/vuln/detail/cve-2026-109618
- CVE-2026-109619 - https://nvd.nist.gov/vuln/detail/cve-2026-109619

Resolution

- **The resolution below is applicable to Avaya Experience Portal 8.1.2.x:**
  1. Download the latest AVL, PHP2Shell Hotfix, and respective README from https://support.avaya.com/support/en/download/AVL_Patch_8.1.2.x?productId=P0407&releaseId=8.1.x
  2. Upgrade to the supported AVL Patch 2607 or 2609; skip if already installed
  3. Apply PHP2Shell Hotfix (PHP_Hotfix_2610.tar.gz) by following instructions in the README

- **The resolution below is applicable to Avaya Experience Portal 8.1.1:**
  1. Download the latest AVL, PHP2Shell Hotfix, and respective README from https://support.avaya.com/support/en/download/AVL_Patch_8.1.x?productId=P0407&releaseId=8.1.x
  2. Upgrade to the supported AVL Patch 2605; skip if already installed
  3. Apply PHP2Shell Hotfix (PHP_Hotfix_2610.tar.gz) by following instructions in the README

- **The resolution below is applicable to Avaya Experience Portal 8.1.0:**
  1. Download the supported AVL, PHP2Shell Hotfix, and respective README from https://support.avaya.com/support/en/download/AVL_Patch_8.0.0-8.1.0?productId=P0407&releaseId=8.1.x
  2. Upgrade to the supported AVL Patch 2502; skip if already installed
  3. Apply PHP2Shell Hotfix (PHP_Hotfix_2610.tar.gz) by following instructions in the README

- **Customers on Avaya Enterprise Portal versions 8.0** – should upgrade to the latest release and follow the Resolution Steps mentioned above. To upgrade to Avaya Experience Portal 8.1 or later, please follow the documentation at https://support.avaya.com/css/en/public/documents/101096779

Workaround or alternative remediation

n/a

Remarks

This Hotfix is not applicable to AEP “Software Only” Solutions. AEP “Software Only” customers should source remediation from their OS providers.

Backup before applying the patch	
Take a snapshot of the system	
Packages	
n/a	
Patch install instructions	**Service-interrupting?**
Follow the README.	YES
Verification	
Follow the README.	
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
https://nvd.nist.gov/vuln/detail/cve-2026-109618 https://nvd.nist.gov/vuln/detail/cve-2026-109619
Avaya Security Vulnerability Classification
None
Mitigation
Follow the Resolution steps

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 LLC, 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.

All trademarks identified by ® or ™ are registered trademarks or trademarks, respectively, of Avaya LLC.
All other trademarks are the property of their respective owners.