Date: October 6, 2026

Revision	Date	Changes
1.0	October 6, 2026	Initial release
1.1	October 13, 2026	Updated Resolution section to include the 2026.3.0 release

The CVE-ID tracking this issue: CVE-2026-101158
CVSSv3.1 Base Score: 8.4 (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H)
CVSSv4.0 Base Score: 9.3
(CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:A/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H)
Common Weakness Enumeration: CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
This vulnerability is being tracked by BUG 1867488

Description

The vulnerability affects both CloudVision Portal (on-premises) and CloudVision-CUE (on-premises). CV-CUE is Arista's Wi-Fi management service and, in on-premises deployments, is hosted as a service on the CloudVision Portal on-premises platform. Because the affected component is used by both product deployments, customers running either CVP or CV-CUE should review the affected versions to assess their impact.

A missing input validation vulnerability in the Fileserver upload API allows an authenticated attacker with file upload privileges to execute stored cross-site scripting (XSS). Successful exploitation could enable the attacker to hijack another CloudVision user's web session, potentially granting full access to their account and administrative permissions.

This issue was discovered internally by Arista, and the company is not aware of any malicious exploitation of this vulnerability in customer networks.

Note: CloudVision as-a-Service and CloudVision CUE cloud service delivery is not impacted by this issue.

Vulnerability Assessment

Platform and Software Applicability Note

To determine actual exposure, operators should first check their software versions against the "Affected Software" list below. If your software release is not listed, your deployment is not vulnerable, regardless of the hardware platform in use.

Affected Software

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

CloudVision Portal Versions

- 2026.2.0
- 2026.1.2 and below releases in the 2026.1.x train
- 2025.3.3 and below releases in the 2025.3.x train
- All prior releases

Note: All CloudVision-CUE (on-premises) versions that ship with the above affected CloudVision Portal (on-premises) versions are also affected.

Affected Platforms

The following products **are** affected by this vulnerability:

- CloudVision Portal on-premises, virtual appliance or physical appliance (including the CV-CUE on premises software)

The following product versions and platforms **are not** affected by this vulnerability:

- Arista EOS-based products:
  - 710 Series
  - 720D Series
  - 720XP/722XPM Series
  - 750X Series
  - 7010TX Series
  - 7020R/R4 Series
  - 7130 Series running EOS
  - 7170 Series
  - 7050X3/X4 Series
  - 7060X/X2/X4/X5/X6 Series
  - 7260X/X3 Series
  - 7280R/R2/R3/R4 Series
  - 7300X/X3 Series
  - 7320X Series
  - 7358X4 Series
  - 7368X4 Series
  - 7388X5 Series
  - 7500R/R2/R3 Series
  - 7800R3/R4 Series
  - 7700R4 Series
  - AWE 5000 Series
  - AWE 7200R Series
  - ZTX-7200 Series
  - CloudEOS

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

    - cEOS-lab
    - vEOS-lab
    - CloudVision eXchange, virtual or physical appliance
- Wi-Fi Access Points
- CloudVision CUE cloud service delivery
- CloudVision Appliance Software
- CloudVision as-a-Service
- CloudVision AGNI - Cloud service delivery
- CloudVision AGNI - Virtual or physical appliance
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric (formerly Big Switch BCF)
- DANZ Monitoring Fabric (DMF) - Controller Appliance
- DANZ Monitoring Fabric (DMF) - Analytics Node Appliance
- DANZ Monitoring Fabric (DMF) - Recorder Node Appliance
- DANZ Monitoring Fabric (DMF) - Service Node Appliance
- Arista Multi Cloud Director (formerly Big Switch MCD)
- Arista Network Detection and Response (NDR) Security Platform (Formerly Awake NDR)
- Arista Edge Threat Management - Arista NG Firewall and Arista Micro Edge (Formerly Untangle)
- Arista NetVisor OS, Arista NetVisor UNUM, and Insight Analytics (Formerly Pluribus)
- VeloCloud Orchestrator (Formerly VeloCloud Orchestrator by Broadcom)
- VeloCloud Gateway (Formerly VeloCloud Gateway by Broadcom)
- VeloCloud Edge (Formerly VeloCloud Edge by Broadcom)

Required Configuration for Exploitation

No specific configuration is required to be vulnerable to this issue. This vulnerability is present in the default configuration of affected releases.

Indicators of Compromise

No indicators of compromise exist.

Mitigation

There is no mitigation available for this vulnerability. However, operators should ensure that roles with file upload permissions are restricted to trusted users.

To do this, review any role that has “**Read and Write**” permission on the following resources, and ensure that only trusted users are assigned to it:

- Bug Alert Management
- File
- Packaging
- Image Repository

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

1. Navigate to **Settings ? Roles**, then click on the "**Pencil**" icon beside a role to edit it.

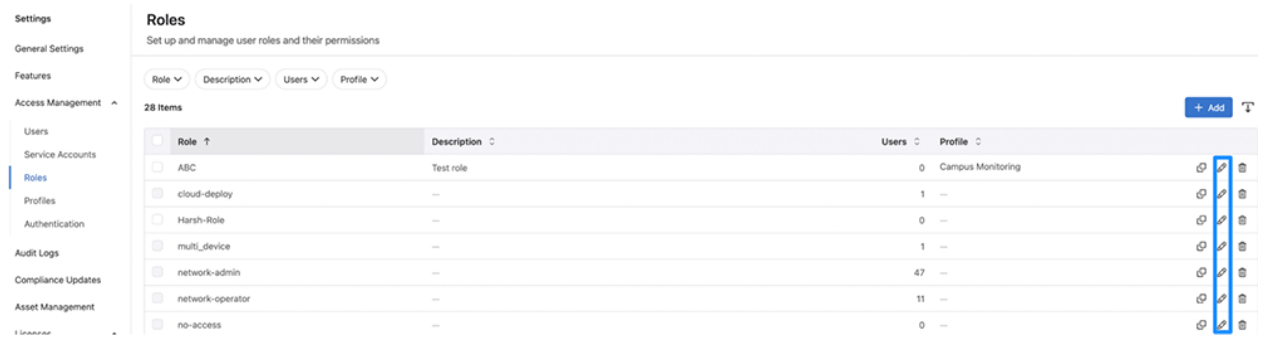

Fig 1: Roles settings page

2. Identify any role that has “**Read and Write**” permission on the resources listed above.

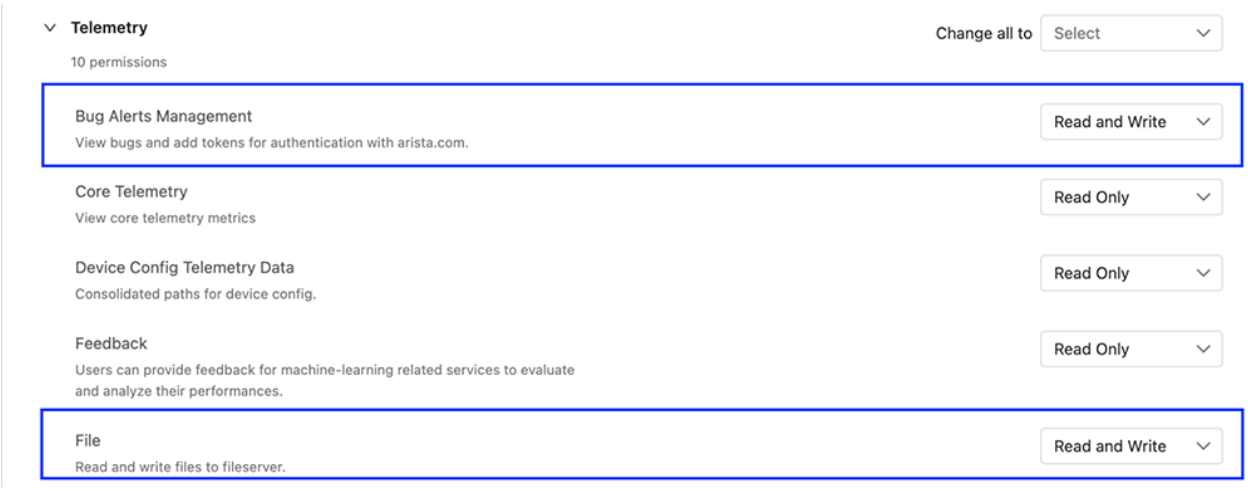

Fig 2: Bug Alerts Management & File



Fig 3: Packaging

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

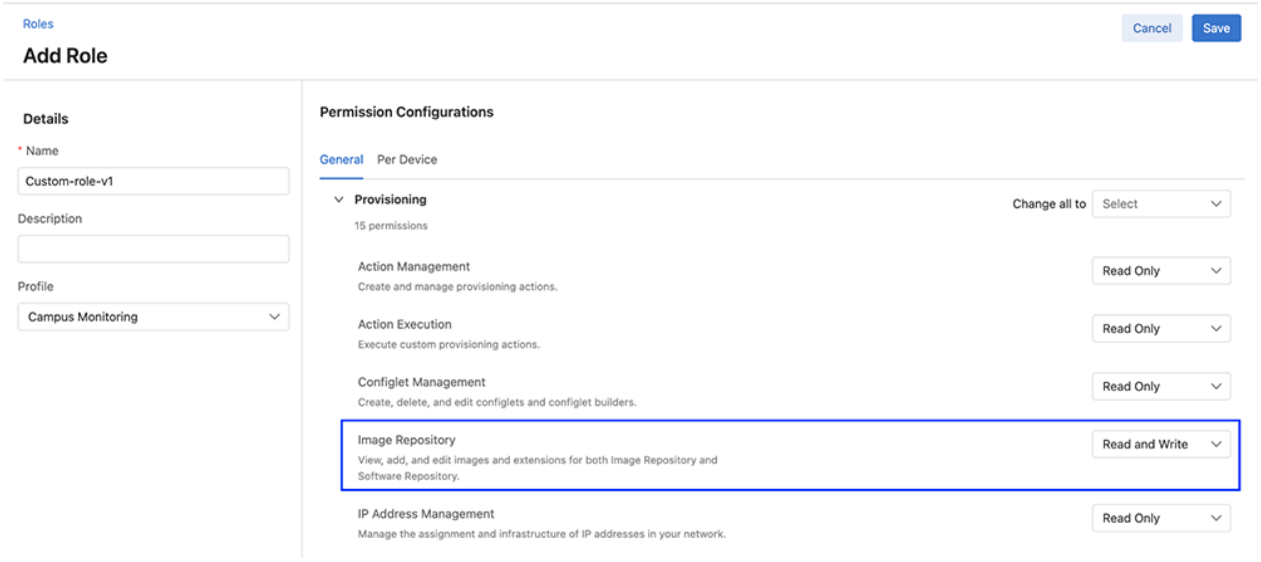

Fig 4: Image Repository

3. Navigate to **Settings ? Users** and verify that only trusted users are assigned to those roles.

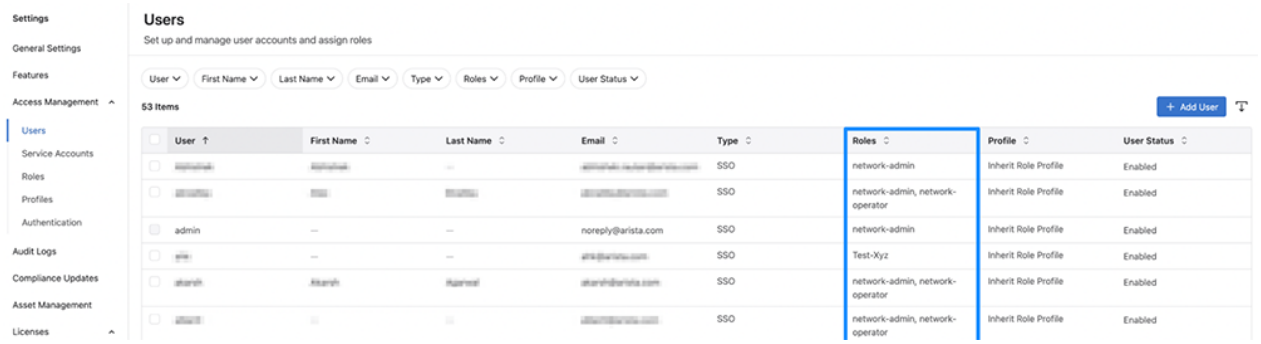

Fig 5: Users settings page

Resolution

The recommended resolution is to upgrade to a remediated software version at your earliest convenience. Arista recommends customers move to the latest version of each release that contains all the fixes listed below. For more information about upgrading see CloudVision Users Manual: Upgrade.

CloudVision Portal and CloudVision CUE

CVE-2026-101158 has been fixed in the following releases:

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

- 2026.3.0 and later releases in the 2026.3.x train
- 2026.2.1 and later releases in the 2026.2.x train
- 2026.1.3 and later releases in the 2026.1.x train
- 2025.3.4 and later releases in the 2025.3.x train

Hotfix

No Hotfix is available for this issue

For More Information

If you require further assistance, or if you have any further questions regarding this security notice, please contact the Arista Networks Technical Assistance Center (TAC) by one of the following methods:

Open a Service Request

Contact information needed to open a new service request may be found at:
https://www.arista.com/en/support/customer-support

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.