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

Description

All CVEs covered in this advisory affect platforms running CloudVision Portal (On-Premises), where insufficient validations in the Software Management Studio Software Repository and the Network Provisioning Image Repository could allow an authenticated remote attacker with specific permissions to read or write files on the platform file system beyond the intended scope through specially crafted requests and/or crafted file uploads.

The below issues were discovered internally by Arista, and the company is not aware of any malicious exploitation of these vulnerabilities in customer deployments.

CVE-2026-101154

An authenticated remote attacker with specific permissions can read or write files on the platform filesystem beyond the intended scope through specially crafted requests and/or crafted file uploads to the Network Provisioning Image Repository.
CVSSv3.1 Base Score: 7.2 (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)
CVSSv4.0 Base Score: 8.6
(CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
This vulnerability is being tracked by BUG 1898843

CVE-2026-101155

An authenticated remote attacker with specific permissions can read or write files on the platform filesystem beyond the intended scope through specially crafted requests and/or crafted file uploads to the Software Management Studio Software Repository.
CVSSv3.1 Base Score: 9.1 (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H)
CVSSv4.0 Base Score: 8.6
(CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
This vulnerability is being tracked by BUG 1898846

Vulnerability Assessment

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.

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

CloudVision Portal Versions

CVE-2026-101154

The following releases are affected:

- 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 back to and including 2018.1.0

CVE-2026-101155

The following releases are affected:

- 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 back to and including 2024.2.0

Affected Platforms

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

- CloudVision Portal, virtual appliance or physical appliance (Note: CV-CUE on-premises is not affected)

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

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.

    - 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
    - cEOS-lab
    - vEOS-lab
    - CloudVision eXchange, virtual or physical appliance
- Wi-Fi Access Points
- CloudVision CUE, virtual appliance or physical appliance
- 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

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.

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.

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.

CVE-2026-101154 and CVE-2026-101155 have been fixed in the following releases:

- 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 exists for these vulnerabilities.

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.