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-2026-101153
CVSSv3.1 Base Score: 8.0 (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H)
CVSSv4.0 Base Score: 7.2
(CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:N/VC:H/VI:N/VA:N/SC:H/SI:H/SA:H)
Common Weakness Enumeration:CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
This vulnerability is being tracked by BUG 1898011

Description

On affected versions of CloudVision Portal (on-premises) or CloudVision Sensor, a path traversal vulnerability exists. An authenticated user with sufficient high privileges could exploit this to extract unintended data from the Sensor.

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

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

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.
- 2025.2.3 and below releases in the 2025.2.x train.
- 2025.1.4 and below releases in the 2025.1.x train.
- 2024.3.3 and below releases in the 2024.3.x train.

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 Sensor Versions

- 1.4.2 and below releases in the 1.4.x train.
- 1.3.1 and below releases in the 1.3.x train.
- All prior releases

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)
- CloudVision Sensor

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

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 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

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

There are no reliable indicators of compromise available for this issue.

Mitigation

There is no reliable mitigation other than stopping the “sensor” component completely, which would prevent all functionality dependent on it from working. This includes any data sources onboarded on that sensor including related telemetry data, as well as functionality such as Universal Network Observability (UNO) and Multi-Domain Segmentation Services (MSS).

To stop the sensor, execute the following command on the CloudVision or Sensor VM:

```
# Stop sensor completely:
cvpi stop sensor
```

To undo this and to start the sensor again use:

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.

```
# Start sensor:
cvpi start sensor
```

Note: While the sensor component is stopped, the sensor and its associated data sources will report as "inactive" in CloudVision.

The recommended resolution is to upgrade to a fixed software version. Make sure to start the sensor component before the upgrade.

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 the Sensor Upgrade section and the CloudVision Upgrade section for your appropriate version.

CloudVision Portal

CVE-2026-101153 has 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

Post-upgrade: It is recommended that the CA cert be rotated, please follow the instructions in CV Helpcenter: Certificate Authority Rotation.

CloudVision Sensor

CVE-2026-101153 has been fixed in the following releases:

- 1.4.3 and later releases in the 1.4.x train

Hotfix

There is no hotfix 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:

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.

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.