Date: October 6, 2026

Revision	Date	Changes
1.0	October 6, 2026	Initial release

Description

All of the CVEs covered in this advisory affect only 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. Customers running CV-CUE services should review the affected versions to assess their impact.

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

CVE-2026-101156

A stored cross-site scripting (XSS) vulnerability may allow an authenticated, high-privilege administrator to store malicious content in a configuration. The content may execute in another authenticated user's browser when that user views or compares the affected configuration. Successful exploitation may allow the attacker to act through the victim's authenticated browser session to access sensitive data, modify configurations, or disrupt managed wireless services.

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: 6.2
(CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:A/VC:N/VI:N/VA:N/SC:H/SI:H/SA:H)
Common Weakness Enumeration: CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') — stored variant.
This vulnerability is being tracked by BUG 1782052.

CVE-2026-101157

A stored cross-site scripting (XSS) vulnerability may allow an unauthenticated attacker with adjacent-network access to inject malicious content that executes when an authenticated user views affected content. Successful exploitation may allow the attacker to compromise the victim's authenticated browser session, access sensitive data, modify system state, or disrupt affected services.

CVSSv3.1 Base Score: 8.7 (CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:L)
CVSSv4.0 Base Score: 9.3
(CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:L/SC:H/SI:H/SA:L)
Common Weakness Enumeration: CWE-79: Improper Neutralization of Input During Web Page Generation (DOM-based stored XSS).
This vulnerability is being tracked by BUG 1802841.

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.

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

CVE-2026-101157

- 2026.2.0
- All prior releases back to 2021.2.0

CVE-2026-101156

- 2026.2.0
- All prior releases back to 2025.2.0

Affected Platforms

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

- CloudVision CUE on-premises, virtual appliance or physical appliance (Note: packaged as part of CloudVision Portal 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

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.

    - 7320X Series
    - 7358X4 Series
    - 7368X4 Series
    - 7388X5 Serie
    - 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 cloud service delivery
- CloudVision Portal, virtual appliance or physical appliance
- 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

CVE-2026-101156 and CVE-2026-101157

To be vulnerable to CVE-2026-101156 and CVE-2026-101157, CV-CUE UI must be enabled and running. The status can be audited with the command “**cvpi status aware**”. Here is an example output of that command that indicates the system is vulnerable:

```
[root@]# cvpi status aware
```

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.

```
Executing command. This may take some time...
Completed 1/1 discovered actions
primary components total:1 running:1 disabled:0
secondary components total:1 running:1 disabled:0
tertiary components total:1 running:1 disabled:0
```

Indicators of Compromise

No indicators of compromise exist for both issues.

Mitigation

There is no mitigation or workaround available for both issues.

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-2026-101156 and CVE-2026-101157 have been fixed in the following releases:

- 2026.2.1 and later releases

Hotfix

No hotfix available for those 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.