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.

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

CVE-2026-102159

An access-control flaw in the CV-CUE backend may allow an unauthenticated network attacker to access functionality intended only for internal services. Successful exploitation may expose sensitive location information or disrupt affected services.
CVSSv3.1 Base Score: 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVSSv4.0 Base Score: 9.3
(CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-306: Missing Authentication for Critical Function
This vulnerability is being tracked by BUG 1732043

CVE-2026-102155

An XML External Entity (XXE) injection vulnerability in the WiFi-server Spectralight application allows any authenticated user to send malicious requests, leading to arbitrary local file disclosure and partial denial of service.
CVSSv3.1 Base Score: 8.5 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:L)
CVSSv4.0 Base Score: 7.1
(CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:L/SC:L/SI:N/SA:N)
Common Weakness Enumeration: CWE-611: Improper Restriction of XML External Entity Reference
This vulnerability is being tracked by BUG 1728574 and BUG 1728163

CVE-2026-102157

An insecure direct object reference (IDOR) vulnerability in a CloudVision CUE file-serving interface may allow an authenticated network user, under specific attack conditions, to access another user's transient data.
CVSSv3.1 Base Score: 5.9 (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:L)
CVSSv4.0 Base Score: 6.8

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.

(CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:N/VA:L/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-639: Authorization Bypass Through User-Controlled Key
This vulnerability is being tracked by BUG 1728161

CVE-2026-102158

Improper validation of selected CloudVision CUE application programming interface (API) request parameters may allow an authenticated network user to perform SQL injection against the backend impacting its availability.
CVSSv3.1 Base Score: 6.5 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)
CVSSv4.0 Base Score: 7.1
(CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component
This vulnerability is being tracked by BUG 1731886

CVE-2026-102160

An operating system (OS) command injection vulnerability in CloudVision CUE backup management may allow an authenticated Super User to submit a crafted backup request and execute arbitrary commands with the privileges of the affected service.
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-78: Improper Neutralization of Special Elements used in an OS Command
This vulnerability is being tracked by BUG 1728182

CVE-2026-102161

An unauthenticated attacker located on an adjacent private network (or any attacker routed through a reverse proxy/load balancer that forwards client headers) can forge their source IP address and gain an administrative session privileges on the CV-CUE backend
CVSSv3.1 Base Score: 8.8 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVSSv4.0 Base Score: 8.7
(CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-798: Use of Hard-coded Credentials, CWE-290: Authentication Bypass by Spoofing
This vulnerability is being tracked by BUG 1728203

Vulnerability Assessment

Platform and Software Applicability Note

To determine actual exposure, operators should first check their software versions against the

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.

"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-2026-102155, CVE-2026-102157, CVE-2026-102160, CVE-2026-102161

- 2026.2.0
- All prior releases back to 2021.2.0

CVE-2026-102158

- 2026.2.0
- All prior releases back to 2022.2.0

CVE-2026-102159

- 2026.2.0
- All prior releases back to 2022.3.0

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

To be vulnerable to CVE-2026-102159, CVE-2026-102155, CVE-2026-102157, CVE-2026-102160, and CVE-2026-102161, CV-CUE backend (wifimanager) must be enabled and running. Here is an example of the command to inspect the status of wifimanager:

```
[root@]# cvpi status wifimanager
Executing command. This may take some time...
Completed 1/1 discovered actions
```

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.

```
primary components total:1 running:1 disabled:0
```

Indicators of Compromise

CVE-2026-102159 and CVE-2026-102155 and CVE-2026-102157 and CVE-2026-102161

No indicators of compromise exist.

CVE-2026-102158

There is no direct indicator of compromise for this issue. Please contact support if suspicious activity patterns are found in the system, as mentioned below.

Too many API calls with long durations logged in the **envoy_https_access.log** file may indicate a compromise. Following commands, which need to be run from the CV-CUE shell, can help find the number of API calls that take more than 5 seconds in the last 1000 calls:

```
[root@19f5761a4950 /]# tail -1000 /opt/wibhu/spectraguard/log/envoy_https_access.log
| awk '  } END '
```

Here is a sample output of the command showing there are 10 slow requests:

```
Slow requests count 10
```

Additionally, a number of API calls with HTTP status 503 can also indicate potential compromises. There is a command to check the count for each HTTP status logged in **envoy_https_access.log**:

```
[root@19f5761a4950 /]# tail -1000 /opt/wibhu/spectraguard/log/envoy_https_access.log
| awk ' $/)  } END  %d\n", c, count[c] } }'
```

Here is a sample output showing that there are 10 API calls with HTTP status 503:

```
Count for  576
Count for  4
Count for  2
Count for  10
Count for  2
Count for  12
```

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.

```
Count for  10
```

CVE-2026-102160

Parameters containing Linux-command-like text, e.g “**cd**”, “**id**”, “**ls**”, etc., from UI operations, logged in **db_ops_ui.log** under **/opt/wibhu/spectraguard/log/**, can indicate a compromise. Please contact support support when suspicious log entries are found in the system.

The log folder can be found with following commands, when run from CVP shell:

```
[root@]# nerdctl exec -it wifimanager -- bash
[root@]# cd /opt/wibhu/spectraguard/log
```

Mitigation

There is no mitigation or workaround available for all 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.

All the CVEs 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:

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.

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.