Date: April 15, 2025

Revision	Date	Changes
1.0	April 15, 2025	Initial release

The CVE-ID tracking this issue: CVE-2024-11186
CVSSv3.1 Base Score: 9.9 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)
Common Weakness Enumeration: CWE-284 Improper Access Control
This vulnerability is being tracked by BUG 1029707

Description

On affected versions of the CloudVision Portal, improper access controls could enable a malicious authenticated user to take broader actions on managed EOS devices than intended. This advisory impacts the Arista CloudVision Portal products when run on-premise. It does not impact CloudVision as-a-Service.

The issue was discovered internally by Arista. Arista is not aware of any malicious uses of this issue in customer networks.

Vulnerability Assessment

Affected Software

CloudVision Versions

- 2024.3.0 and below releases in the 2024.3.x train
- 2024.2.1 and below releases in the 2024.2.x train
- 2024.1.2 and below releases in the 2024.1.x train
- All releases in the 2023.3.x train
- All releases in the 2023.2.x train
- All releases in the 2023.1.x train
- All releases in the 2022.3.x train
- All releases in the 2022.2.x train
- All releases in the 2022.1.x train
- All releases in the 2021.3.x train
- All releases in the 2021.2.x train
- All releases in the 2021.1.x train
- All releases in the 2020.3.x train
- All releases in the 2020.2.x train
- All releases in the 2020.1.x train
- All releases in the 2020.3.x train
- All releases in the 2020.2.x train
- All releases in the 2020.1.x train
- All releases in the 2019.1.x train

- All releases in the 2018.2.x train
- All releases in the 2018.1.x train
- All releases in the 2017.2.x train

Affected Platforms

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

- CloudVision Portal, virtual appliance or physical appliance

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
    - 7010 Series
    - 7010X Series
    - 7020R Series
    - 7130 Series running EOS
    - 7150 Series
    - 7160 Series
    - 7170 Series
    - 7050X/X2/X3/X4 Series
    - 7060X/X2/X4/X5/X6 Series
    - 7250X Series
    - 7260X/X3 Series
    - 7280E/R/R2/R3 Series
    - 7300X/X3 Series
    - 7320X Series
    - 7358X4 Series
    - 7368X4 Series
    - 7388X5 Series
    - 7500E/R/R2/R3 Series
    - 7800R3 Series
    - CloudEOS
    - cEOS-lab
    - vEOS-lab
    - AWE 5000 Series
    - AWE 7200R Series
- Arista Wireless Access Points

- CloudVision as-a-Service
- CloudVision CUE, virtual appliance or physical appliance
- CloudVision CUE cloud service delivery
- CloudVision eXchange, virtual or physical appliance
- CloudVision AGNI
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric and DANZ Monitoring Fabric (Formerly Big Switch Nodes for BCF and BMF)
- 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)

Required Configuration for Exploitation

In order to be vulnerable to CVE-2024-11186, the following condition must be met:

- A user must be able to authenticate with CloudVision

Indicators of Compromise

All CLI commands sent to devices are logged in by the device-interaction app in lines that start with “Request to execute:”. These logs along with device Radius/TACACS logs can be checked for suspicious activity.

Mitigation

The workaround is to append the following to /etc/nginx/conf.d/locations/cvp.https.conf on all CVP nodes:

```
location ^~ /cvpservice/di/ {
    return 404;
}
```

Then restart nginx by running the following command on any node:

```
nginx-app.sh reload
```

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 Guide.

CVE-2024-11186 has been fixed in the following releases:

- 2025.1.0 and later releases in the 2025.1.x train
- 2024.3.1 and later releases in the 2024.3.x train
- 2024.2.2 and later releases in the 2024.2.x train
- 2024.1.3 and later releases in the 2024.1.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