Date: March 7, 2023

Revision	Date	Changes
1.0	March 7, 2023	Initial release

The CVE-ID tracking this issue: CVE-2023-24546

CVSSv3.1 Base Score: 10.0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:L)

Note: This issue has been filed on MITRE as having a CVSS score of 10.0. Depending on the release and configuration there is some variance on the Base Score. The range of possible CVSS scores and mapping to the releases is detailed in the “Required Configuration for Exploitation” section below.

Common Weakness Enumeration: CWE-284: Improper Access Control

This vulnerability is being tracked by BUG 756614

Description

On affected versions of the CloudVision Portal, improper access controls on the connection from devices to CloudVision could enable a malicious actor with network access to CloudVision to get broader access to telemetry and configuration data within the system than intended. This advisory impacts the Arista CloudVision Portal products when run on-premise. It does not impact CloudVision as-a-Service.

Vulnerability Assessment

Affected Software

CloudVision Portal Versions

- All releases in the 2021.1 train
- All releases in the 2021.2 train
- All releases in the 2021.3 train
- 2022.1.0
- 2022.1.1
- 2022.2.0
- 2022.2.1
- 2022.3.0

Note: CloudVision Portal versions prior to 2021.1.0 are not impacted.

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:
    - 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 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
- Arista Wireless Access Points
- CloudVision WiFi, virtual appliance or physical appliance
- CloudVision WiFi cloud service delivery
- CloudVision as-a-Service
- 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 - Formerly Untangle (Formerly Arista NG Firewall and Arista Micro Edge)
- Arista Unified Cloud Fabrics - (Formerly Pluribus Netvisor One)

Required Configuration for Exploitation

All versions of CloudVision listed in the “Affected Software” section above are vulnerable to CVE-2023-24546 but the degree of severity varies based on the current version of CloudVision and the original version of CloudVision used to deploy the cluster.

In the 2021.1 and 2021.2 releases, a bug in the authorization layer gave certain types of clients read access to additional parts of the CloudVision database, including CloudVision configuration settings. In these releases the CVSS score is **7.6** (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L).

In the 2021.3 train, 2022.1.0, 2022.1.1, 2022.2.0, 2022.2.1, and 2022.3.0 releases, there was a further bug in the authorization layer giving those same clients write access to additional parts of the CloudVision database. In these releases the CVSS score is **9.9** (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:L).

For clusters that were first deployed with the 2022.2.0 or 2022.2.1 releases, the CVSS score is **10.0** (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:L) due to an additional issue.

The overall impact is that a malicious actor with network access to the CloudVision cluster and the credentials for a specific type of account could read or write additional state in the CloudVision database, including telemetry and configuration state.

Indicators of Compromise

There are no indications of compromise.

Mitigation

There are no mitigation steps. Please upgrade to a fixed version.

Resolution

The resolution is to upgrade to a remediated software version. Arista recommends customers move to the latest version of each release that contains all the fixes listed below.

CVE-2023-24546 has been fixed in the following releases:

- 2022.1.2
- 2022.2.2
- 2022.3.1

Hotfix

No hotfix is available.

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

By email: support@arista.com

By telephone: 408-547-5502 ; 866-476-0000

Contact information needed to open a new service request may be found at:

https://www.arista.com/en/support/customer-support