Date: April 15, 2025

Revision	Date	Changes
1.0	April 15, 2025	Initial release

The CVE-ID tracking this issue: CVE-2025-0505
CVSSv3.1 Base Score: 10.0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N)
Common Weakness Enumeration:CWE- CWE-269: Improper Privilege Management
This vulnerability is being tracked by BUG 1046170

Description

On Arista CloudVision systems (virtual or physical on-premise deployments), Zero Touch Provisioning can be used to gain admin privileges on the CloudVision system, with more permissions than necessary, which can be used to query or manipulate system state for devices under management. Note that CloudVision as-a-Service is not affected.

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 Portal Versions

- 2024.2.0 and 2024.2.1
- 2024.3.0

Note: All CV-CUE (on-premise) versions that ship with the above affected CloudVision Portal (on-premise) versions are also affected.

Affected Platforms

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

- CloudVision Portal, virtual appliance or physical appliance
- CloudVision CUE, virtual appliance or physical appliance

The following product versions and platforms **are not** affected by this vulnerability:

- Arista EOS-based products:

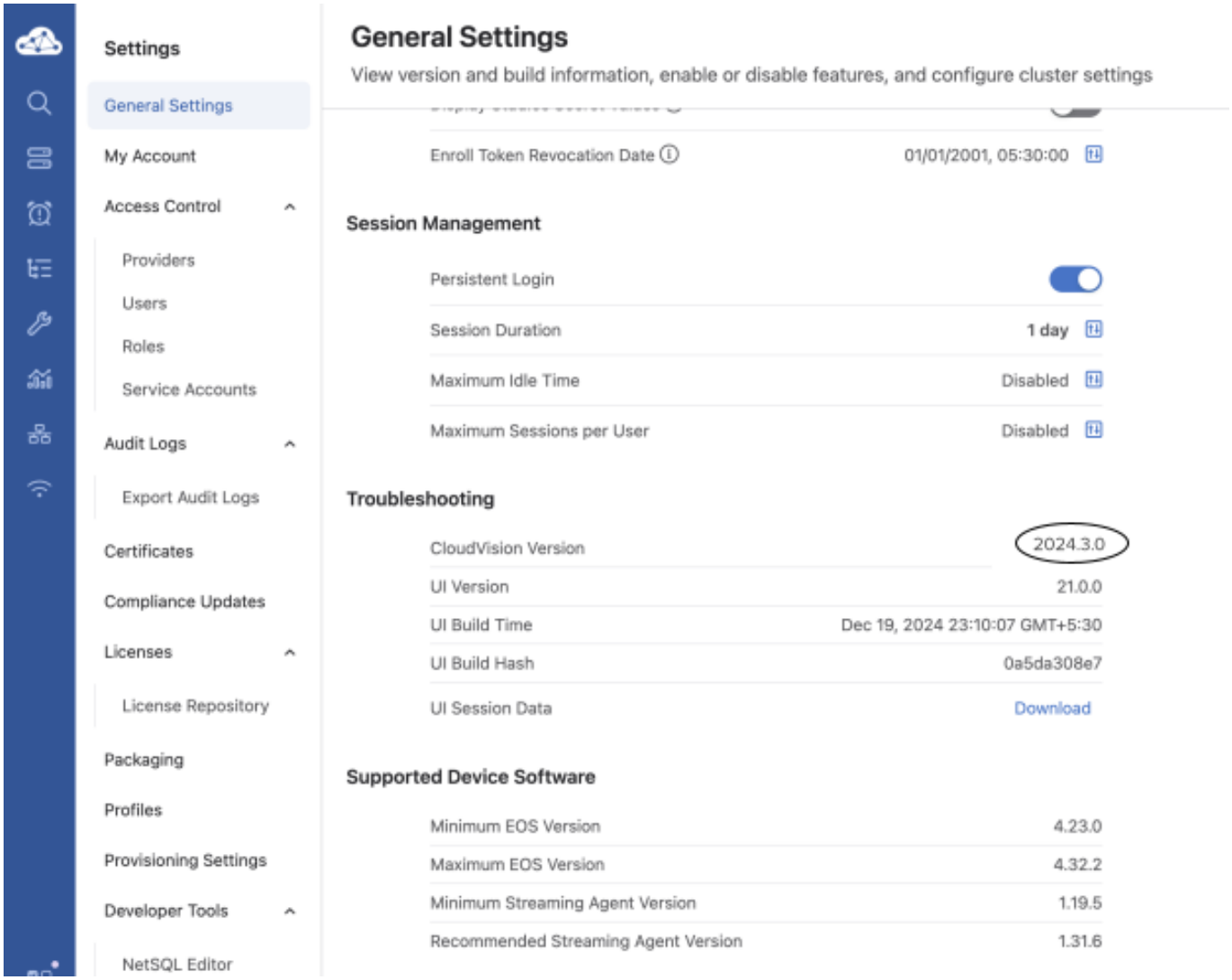
    - 710 Series
    - 720D Series
    - 720XP/722XPM Series
    - 750X Series
    - 7010 Series
    - 7010X Series
    - 7020R Series
    - 7130 Series running EOS
    - 7150 Series
    - 7160 Series
    - 7170 Series
    - 7050X/X2/X3/X4 Series
    - 7060X/X2/X4/X5/X6 Series
    - 7250X Series
    - 7260X/X3 Series
    - 7280E/R/R2/R3 Series
    - 7300X/X3 Series
    - 7320X Series
    - 7358X4 Series
    - 7368X4 Series
    - 7388X5 Series
    - 7500E/R/R2/R3 Series
    - 7700R4 Series
    - 7800R3/R4 Series
    - CloudEOS
    - cEOS-lab
    - vEOS-lab
    - AWE 5000 Series
    - AWE 7200R Series
- Arista Wireless Access Points
- CloudVision CUE cloud service delivery
- CloudVision eXchange, virtual or physical appliance
- CloudVision as-a-Service
- 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

Zero Touch Provisioning is enabled by default on CloudVision Portal, as such there are no

configuration settings specific to this vulnerability.

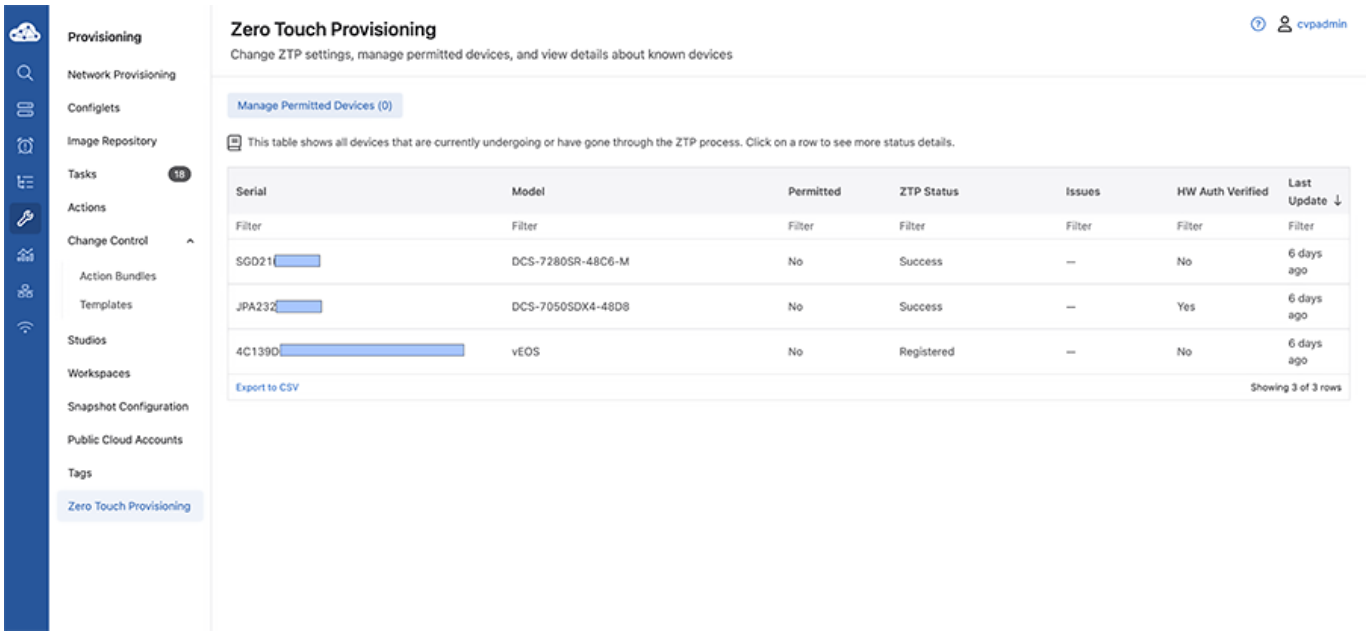
The CloudVision versions listed in the “Affected Software” section above are vulnerable. In order to determine your software version, navigate to the Settings page on the CloudVision UI.



Indicators of Compromise

The Zero Touch Provisioning screen shown in the image below can be used to check for suspicious or unexpected device serial numbers. They could be:

- A device serial that the customer does not own
- A device serial that is known to not have been provisioned using ZTP



Mitigation

The ZTP component on CloudVision (on-premise) can be disabled by running the following on any of the nodes of the CloudVision deployment (Note that this will disable the Zero Touch Provisioning feature on CloudVision):

```
cvpi disable ztp
cvpi stop ztp
```

The following command can be used to verify that the component is stopped:

```
cvpi status ztp

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

The component may be enabled after upgrading to one the remediated software versions (See Resolution) using the following commands:

```
cvpi enable ztp
cvpi start ztp
```

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 Upgrade | Setup Guide | Arista CloudVision 2024.3 Help Center

CVE-2025-0505 has been fixed in the following releases:

- 2024.2.2 and later releases in the 2024.2.x train
- 2024.3.1 and later releases in the 2024.3.x train

Hotfix

No hotfix is available. Please upgrade to a remediated software version.

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