Date: April 15, 2025

Revision	Date	Changes
1.0	April 15, 2025	Initial release

The CVE-ID tracking this issue: CVE-2024-8100
CVSSv3.1 Base Score: 8.7 (CVSS:3.1AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N)
Common Weakness Enumeration: CWE-269: Improper Privilege Management
This vulnerability is being tracked by BUG 994965

Description

On affected versions of the Arista CloudVision Portal (CVP on-prem), the time-bound device onboarding token can be used to gain admin privileges on CloudVision.

This vulnerability was discovered internally and Arista is not aware of any malicious uses of this issue in customer networks.

Vulnerability Assessment

Affected Software

CVP Versions

- 2024.3.0
- 2024.2 and below releases in the 2024.x train
- 2023.3.1 and below releases in the 2023.3.x train
- 2023.2 and below releases in the 2023.x train
- All releases in the 2022.x, 2021.x, 2020.x, 2019.x, and 2018.x trains

Affected Platforms

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

- CloudVision Portal

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/R4 Series
    - 7700R4 Series
    - CloudEOS
    - cEOS-lab
    - vEOS-lab
    - AWE 5000 Series
    - AWE 7200R Series
- Arista Wireless Access Points
- 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)
- CloudVision as-a-Service
- CloudVision AGNI
- CloudVision CUE, virtual appliance or physical appliance
- CloudVision CUE cloud service delivery
- CloudVision eXchange, virtual or physical appliance

Required Configuration for Exploitation

No specific configuration is required to be vulnerable to CVE-2024-8100.

Indicators of Compromise

No indicators of compromise exist.

Mitigation

Best practice is for generated device onboarding tokens to be valid for a limited time duration, and for the Device Onboarding permission which allows the generation of these tokens to only be granted to trusted users.

Successful exploit generally requires one of the following:

1. A rogue or compromised internal user with Device enrollment read/write permissions

OR,

2. A valid device onboarding token that is easily accessible beyond the expected set of trusted users

If all users with Device Onboarding privileges are trusted, and onboarding tokens are properly secured, then the risk of this issue is limited.

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 CVP Software downloads

CVE-2024-8100 has been fixed in the following releases:

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

Hotfix

No Hotfix exists 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