Date: September 22, 2026

Revision	Date	Changes
1.0	September 22, 2026	Initial release
1.1	September 23, 2026	CSAF JSON file added

The CVE-ID tracking this issue: CVE-2026-93952
CVSSv3.1 Base Score: 10.0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CVSSv4.0 Base Score: 9.5
(CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H)
Common Weakness Enumeration: CWE-20: Improper Input Validation
This vulnerability is being tracked by BUG1907167, and BUG1937417.

Description

VeloCloud Orchestrator (VCO) on-prem has a security issue where this issue may allow a remote attacker to access privileged internal functionality and impact the VCO host. Successful exploitation may compromise the confidentiality, integrity, and availability of the orchestrator and data managed by the orchestrator.

Hosted, including Dedicated, versions of VCO were impacted and have already been patched.

This issue was discovered externally and is known to be actively exploited.

Vulnerability Assessment

Platform and Software Applicability Note

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

VeloCloud Orchestrator (VCO) Versions

- 5.2.3.15 and below releases in the 5.2.x train
- 6.1.3.7 and below releases in the 6.1.x train
- 6.4.2.7 and below releases in the 6.4.x train
- 7.0.0.2 and below releases in the 7.0.x train.

Affected Platforms

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

- VeloCloud Orchestrator On-Prem (Formerly VeloCloud Orchestrator by Broadcom)

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
  - 7320X Series
  - 7358X4 Series
  - 7368X4 Series
  - 7388X5 Serie
  - 7500R/R2/R3 Series
  - 7800R3/R4 Series
  - 7700R4 Series
  - AWE 5000 Series
  - AWE 7200R Series
  - CloudEOS
  - cEOS-lab
  - vEOS-lab
  - CloudVision eXchange, virtual or physical appliance
- Wi-Fi Access Points
- CloudVision CUE, virtual appliance or physical appliance
- 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 Gateway (Formerly VeloCloud Gateway by Broadcom)
- VeloCloud Edge (Formerly VeloCloud Edge by Broadcom)

Required Configuration for Exploitation

VCO is exposed if certificate based authentication from the VeloCloud Edge to VeloCloud Orchestrator (VCO) is configured. Access to the public portion of the VeloCloud Edge authentication certificate is required. A successful attack requires network access to the VCO web interface. VCO tenant or operator credentials are not required for this exposure.

Deployments that restrict VCO web interface access to trusted administrative networks can reduce risk of exposure.

Indicators of Compromise

There is no single definitive indicator of compromise for this issue.

Operators should review VCO web access logs for unexpected activity. Requests containing unusual URL-like path components, encoded characters, references to local or internal services, or high request rates should be investigated.

Operators should also review VCO backend application logs and system logs for activity near the same timestamps. The following may warrant review:

- Incoming requests to the VCO from known malicious IPs
- Unexpected outbound HTTP or HTTPS activity originating from the VCO host
- Sensitive configuration changes that do not correspond to administrator activity
- Privileged maintenance actions that are not associated with expected administrative workflows
- Unexpected command execution, file creation, database export, or archive artifacts on the VCO host
- Unexpected access to VCO database contents, configuration data, device inventory, credentials, certificates, or key material

If the following indicators of compromise are located, please preserve the state of the VCO and reach out to TAC or your account team for further assistance:

- Files
    - /usr/local/sbin/.vcnode.js
    - /usr/local/sbin/vc-sysmond

        - Known malicious hash of file is (md5) “dc78e206eaeadec59fc5801fe4556bd0”
    - /etc/systemd/system/vc-sysmon.service
- The following HTTP header in nginx logs
    - x-vc-opt
- Connections from the following IP addresses
    - 142.93.149.77
    - 104.248.126.159

If compromise is suspected, operators should preserve VCO web access logs, backend application logs, system logs, database logs, and relevant file-system timestamps before remediation where operationally feasible.

Mitigation

The recommended resolution is to upgrade to a fixed VCO release as soon as it is available. For VCOs which are not on a supported release train, customers can contact TAC to discuss possible upgrade options for your release.

Until the fixed software is deployed, operators should apply defense-in-depth controls appropriate for their environment:

- Restrict access to the VCO web interface to trusted administrative networks.
- Monitor the VCO for accesses from known malicious source IPs.
- Monitor for unexpected outbound network activity from the VCO host.
- Consider blocking outbound ports not needed for normal activities.
- Monitor for backdoor daemons and webshells
- Review recent administrator activity for unexpected changes.

Resolution

The recommended resolution is to upgrade to a remediated software version at your earliest convenience. Fixes are coming out for affected release trains under support and will be updated here when ready.

These vulnerabilities have been fixed in the following releases:

- VCO 5.2.3.16 and later in the 5.2.3 train
- VCO 6.4.2.8 and later in the 6.4.2 train

Releases in other release trains that fix this will be added over time.

Post-Remediation Guidance

Because successful exploitation may compromise the orchestrator host and data managed by

the orchestrator, operators should follow incident-response guidance appropriate for their deployment. Compromises to the VCO platform may allow attackers access to the VeloCloud Edge devices as well. This may include credential rotation, review of administrator activity, validation of managed device state, and restoration or replacement of affected orchestrator instances from trusted sources.

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