Date: September 9, 2026

Revision	Date	Changes
1.0	September 9, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-86108
CVSSv3.1 Base Score: 8.0 (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H)
CVSSv4.0 Base Score: 7.5
(CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
This vulnerability is being tracked by BUG1857467, BUG1833895, BUG1833902, BUG1833887.

Description

Insufficient validation of inputs supplied through affected VeloCloud Edge management and configuration workflows may allow an authorized management request or configuration value to be interpreted as an operating-system command. Successful exploitation may allow command execution with elevated privileges on the affected VeloCloud Edge.

This issue was discovered internally by Arista, and the company is not aware of any malicious exploitation of this vulnerability in customer networks.

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 Edge Versions

- 6.4.1.x and below releases in the 6.4.x train
- 6.1.4.x and below releases in the 6.1.x train
- 5.2.6.x and below releases in the 5.2.x.x train
- All prior releases

Affected Platforms

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

- VeloCloud Edge (Formerly VeloCloud Edge 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 Series
  - 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 Orchestrator (Formerly VeloCloud Orchestrator by Broadcom)
- VeloCloud Gateway (Formerly VeloCloud Gateway by Broadcom)

Required Configuration for Exploitation

To successfully leverage this vulnerability, an attacker must either control a compromised VeloCloud Orchestrator or possess the credentials required to submit malicious parameters through an established management interface.

Indicators of Compromise

No reliable, vulnerability-specific indicators of compromise have been identified. Customers should investigate runDiagnostics activity that cannot be matched to authorized troubleshooting, particularly unexpected diagnostic names or parameter values, activity outside an approved maintenance window, or activity associated with an unexpected VCO user. Related Edge log entries can be correlated using the timestamp and action ID. These records are investigative leads and do not independently confirm exploitation. The log formats are captured below.

```
<TIMESTAMP> INFO [websocketclient (...)]
  message received: {?"action":"runDiagnostics","actionId":"<id>","data":
  }

<TIMESTAMP> INFO [live_websocket (...)]
  diag_worker received jobs [[]]

<TIMESTAMP> INFO [diagutils (...)]
  Queuing diagnostic run command: ['/opt/vc/diag/scripts/rundiagnostics.lua',
  'run', '<diagnostic>', '<parameter-json>']
```

Mitigation

Until an upgrade can be completed, customers should:

- Restrict VeloCloud Orchestrator Super Admin and Operator roles, particularly Remote Diagnostics and device-configuration access, to trusted personnel.
- Protect Orchestrator administrative credentials and management access.
- Maintain the default Local UI access restrictions and limit activation access to authorized personnel.

These measures reduce exposure but do not prevent exploitation of the issue.

Resolution

Migrating to a patched software version for VeloCloud Edge is the advised course of action. Arista suggests that operators transition to the most recent release within a supported branch that incorporates the necessary remediations. The vulnerability identified as CVE-2026-86108 is addressed in the following versions:

- 7.0.0 and later releases
- 6.4.2 and later releases in the 6.4.x train
- 6.1.5.0 and later releases in the 6.1.x train
- 5.2.7.0 and later releases in the 5.2.7.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