Date: July 27, 2026

Revision	Date	Changes
1.0	July 27, 2026	Initial release

Description: SQL injection in a flow metrics API method enabling server-side request forgery
CVE: CVE-2026 -17191
CVSSv3.1 Base Score: 9.1 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:L)
CVSSv4.0 Base Score: 8.5
(CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:L/VA:L/SC:H/SI:L/SA:L/S:P)
Common Weakness Enumeration: CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
This vulnerability is being tracked by BUG 1568507

Description: Server-side request forgery due to missing input validation in a feature
CVE: CVE-2026 -17192
CVSSv3.1 Base Score: 8.5 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N)
CVSSv4.0 Base Score: 6.3
(CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:N/SC:H/SI:L/SA:N/S:P)
Common Weakness Enumeration: CWE-918 Server-Side Request Forgery (SSRF)
This vulnerability is being tracked by BUG 1568526

Description

CVE-2026 -17191 — SQL injection enabling server-side request forgery in a VeloCloud Orchestrator (VCO) flow metrics API method

An input validation vulnerability exists in an API component of the orchestrator. An authenticated user can exploit this flaw to manipulate backend queries, which may result in unauthorized access to data beyond their intended privileges and cause the underlying system to initiate unintended outbound network connections.

CVE-2026 -17192 — Server-side request forgery due to missing input validation in a VCO feature

A VCO feature does not sufficiently validate caller-supplied input, allowing requests to be made on behalf of authenticated tenant accounts to internal services that are not otherwise accessible. This vulnerability requires a minimum role of Enterprise Standard Admin.

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

Vulnerability Assessment

Affected Software

VeloCloud Orchestrator (VCO) Versions

- VCO 5.2.x releases prior to 5.2.3.14
- VCO 6.1.x releases prior to 6.1.3.4
- VCO 6.4.x releases prior to 6.4.2.4

Note: End of support software versions have not been assessed.

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
  - 7010 Series
  - 7010X Series
  - 7020R/R4 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/R4 Series
  - 7300X/X3 Series
  - 7320X Series
  - 7358X4 Series
  - 7368X4 Series
  - 7388X5 Series
  - 7500E/R/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
- Arista Wireless Access Points
- CloudVision CUE, virtual appliance or physical appliance
- CloudVision CUE cloud service delivery
- CloudVision Portal, virtual appliance or physical appliance
- CloudVision as-a-Service
- CloudVision AGNI - Cloud service delivery
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric (formerly Big Switch BCF)
- Arista DANZ Monitoring Fabric (formerly Big Switch 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)
- VeloCloud Orchestrator Hosted (Formerly VeloCloud Orchestrator by Broadcom)
- VeloCloud Gateway (Formerly VeloCloud Gateway by Broadcom)
- VeloCloud Edge (Formerly VeloCloud Edge by Broadcom)

Required Configuration for Exploitation

1) CVE-2026-17191 — SQL injection enabling server-side request forgery in a VCO flow metrics API method

A successful attack requires a valid authenticated session on the VCO portal. The minimum user role required is **Enterprise Read Only**, the lowest built-in tenant role. No non-default configuration is required.

2) CVE-2026-17192 — Server-side request forgery due to missing input validation in a VCO feature

A successful attack requires a valid authenticated session on the VCO portal. The minimum role required is **Enterprise Standard Admin**. No non-default configuration is required.

Indicators of Compromise

No reliable indicators of compromise exist.

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.
- Review recent administrator activity for unexpected changes.

Resolution

The recommended resolution is to upgrade to a fixed VCO release at your earliest convenience.

These vulnerabilities have been fixed in the following releases:

- VCO **5.2.3.14** and later in the 5.2 train
- VCO **6.1.3.4** and later in the 6.1 train
- VCO **6.4.2.4** and later in the 6.4 train

Hotfix

No hotfix is available for these issues.

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