Date: September 9, 2026

Revision	Date	Changes
1.0	September 9, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-86107
CVSSv3.1 Base Score: 5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)
CVSSv4.0 Base Score: 8.2
(CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-787 Out-of-bounds Write
This vulnerability is being tracked by BUG 1833888

Description

The VeloCloud Edge and Gateway exhibit an out-of-bounds write vulnerability when processing tunneled IP fragments between authenticated overlay neighbors. This vulnerability impacts the VeloCloud VCMP tunnel protocol only.

A successful exploit can cause the affected process to terminate and restart, leading to a temporary disruption of traffic. Hosts on the internet that are unauthenticated and unable to form an overlay peer relationship can not trigger the vulnerable logic.

These issues were discovered internally by Arista. Arista is not aware of any malicious exploitation of these vulnerabilities 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 Gateway and 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

Affected Platforms

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

- VeloCloud Gateway (Formerly VeloCloud Gateway by Broadcom)
- 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
- Arista Wireless 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)

Required Configuration for Exploitation

No specific configuration is required. Successful exploitation of this vulnerability necessitates that an authenticated VCMP tunnel be established between a target VeloCloud Edge or Gateway and a malicious VeloCloud Edge. Once the relationship is formed, the attacker must transmit specifically malformed fragmented packets.

Indicators of Compromise

No reliable, vulnerability-specific indicators of compromise have been identified.

A successful attack may cause the ‘edged’ process on the VeloCloud Edge or the ‘gwd’ process on the VeloCloud Gateway to restart, but there are no direct indicators the restart was caused by this vulnerability. If observed, customers should collect a diagnostic bundle through the supported VeloCloud Orchestrator diagnostic workflow and contact Arista TAC.

Mitigation

No mitigation is available for this issue.

As a risk-reduction measure, customers should ensure that only trusted and authorized VeloCloud Edges can establish overlay peer relationships, revoke credentials for decommissioned or suspect devices, and isolate any peer that exhibits unexpected IP fragmentation behavior. These measures reduce exposure but do not prevent the vulnerabilities.

Resolution

The recommended resolution is to upgrade to a remediated VeloCloud software version at the earliest opportunity. Arista recommends that customers move to the latest available release in a supported train that contains the fixes.

CVE-2026-86107 has been fixed in the following releases:

- 7.0.0 and later releases
- 6.4.2.0 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