**Date: November 2, 2026**

| Revision | Date | Changes |
|---|---|---|
| 1.0 | November 2, 2026 | Initial release |

The CVE-ID tracking this issue: CVE-2026-111497
CVSSv3.1 Base Score: 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVSSv4.0 Base Score: 9.2
(CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-252 Unchecked Return Value , CWE-787 Out-of-bounds write
This vulnerability is being tracked by BUG 2053049 (VeloCloud Orchestrator)

# Description

This security advisory addresses CVE-2026-111497 (HTTP2Shell), which involves a buffer overflow vulnerability within Google's Brotli C decoder and bundled software versions. A remote, unauthenticated attacker could exploit this issue by supplying a specifically crafted PDU potentially causing a denial of service, exposing sensitive memory, or executing arbitrary code.

Arista Engineering and PSIRT teams are comprehensively reviewing all product lines to identify the products that may be affected by this vulnerability. Arista will continue to update this advisory with possible mitigations and fixed software releases as soon as they are available.

# 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

- 6.4.2.13 and below releases in the 6.4.2 train
- 6.1.3.11 and below releases in the 6.1.3 train
- 5.2.3.19 and below releases in the 5.2.3 train

## Affected Platforms

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

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

- VeloCloud Orchestrator (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 Series
  - 7500R/R2/R3 Series
  - 7800R3/R4 Series
  - 7700R4 Series
  - AWE 5000 Series
  - AWE 7200R Series
  - ZTX-7200 Series
  - CloudEOS
  - cEOS-lab
  - vEOS-lab
  - CloudVision eXchange, virtual or physical appliance
- Wi-Fi Access Points
- CloudVision Portal, virtual appliance or physical appliance (Note: CV-CUE on-premises is undergoing triage)
- CloudVision as-a-Service
- CloudVision AGNI - Cloud service delivery
- CloudVision AGNI - Virtual or physical appliance
- VeloCloud Gateway (Formerly VeloCloud Gateway by Broadcom)

The following product versions and platforms are **undergoing triage** to determine if they are affected by this vulnerability:

- CloudVision CUE cloud service delivery
- CloudVision CUE on-premises, virtual appliance or physical appliance (Note: packaged

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

as part of CloudVision Portal on-premises software)
- CloudVision Appliance Software
- 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 Edge (Formerly VeloCloud Edge by Broadcom)

## Required Configuration for Exploitation

### VeloCloud Orchestrator

Exploitation requires an affected VCO runtime to process a specially crafted Brotli-compressed response through an outbound HTTP client that supports automatic decompression.

This could occur when VCO communicates with an attacker-controlled or compromised integration endpoint, including a destination reached through an HTTP redirect where the client follows redirects. Examples include Broadcom Symantec, Zscaler, and Azure Non SD-WAN Destination (NSD) integrations. Ensure third-party URLs are configured to trusted endpoints. An existing trusted endpoint could be compromised without any change to VCO configuration.

Our assessment to date has not identified Brotli decoding in the reviewed inbound API request paths. Normal use of Brotli compression does not indicate malicious activity.

# Indicators of Compromise

### VeloCloud Orchestrator

No VCO-specific detection signature has been validated in this assessment. Operators should investigate:

- Unexpected VCO service crashes, restarts, or memory-access faults occurring around outbound integration requests.
- Unauthorized changes to integration URLs or unexpected outbound connections to unfamiliar destinations.
- Unexpected process execution, file creation, configuration changes, or access to sensitive data following suspicious integration activity.

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

These observations warrant investigation but are not, individually, proof of exploitation. A Brotli-compressed response alone is not an indicator of compromise, and the absence of crashes does not establish that exploitation has not occurred.

If compromise is suspected, preserve relevant VCO application, system, and audit logs, together with available network records and crash diagnostics. Contact support with the VCO version/build, timestamps, and affected integration details.

## Mitigation

### VeloCloud Orchestrator

There is no mitigation available for this issue.

## 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.

The issue is fixed in the following product releases:

### VeloCloud Orchestrator

- 6.4.2.14 and later releases in the 6.4.2 train
- 6.1.3.12 and later releases in the 6.1.3 train
- 5.2.3.20 and later releases in the 5.2.3 train

### For More Information:

If you require further assistance, or if you have any further questions regarding this notice, please contact the Arista Networks Technical Assistance Center (TAC) by one of the following methods:

- Open a Service Request: https://arista.com
- By email: support@arista.com
- By telephone: +1-408-547-5502, +1-866-476-0000 - more

### Receive Notifications

Subscribe to the RSS feed and email notifications to receive periodic updates on new software releases, end of sale, end of support and field notices

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.