Date: September 9, 2026

Revision	Date	Changes
1.0	September 9, 2026	Initial release
1.1	September 22, 2026	CSAF JSON file added

The CVE-ID tracking this issue: CVE-2026-86109
CVSSv3.1 Base Score: 6.6 (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/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-347: Improper Verification of Cryptographic Signature
This vulnerability is being tracked by BUG1833886.

Description

The VeloCloud Edge software update workflow may accept update bundles without properly validating their signatures because the workflow does not restrict the digest algorithm used for artifact verification. An attacker with either sufficient privileges to upload packages to VeloCloud Orchestrator or credentials permitting direct access to an Edge may be able to install unauthorized software.

This issue was discovered internally by Arista. Arista 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

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.

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
- 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

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.

- 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

Exploitation requires control over the software-update package or associated update metadata delivered to the Edge. This could result from compromise of the VeloCloud Orchestrator or high-privilege access sufficient to stage, replace, or control an Edge software-update package.

Indicators of Compromise

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

Customers should review Orchestrator audit and event history for unexpected VeloCloud Edge software-update operations or unexplained software-version changes. If suspicious update activity is identified, customers should collect a VeloCloud Edge diagnostic bundle and contact Arista TAC.

Mitigation

Until an upgrade can be completed, customers should continue to follow operational best practices, including:

- Restrict software-image management and VeloCloud Edge update privileges to trusted administrators.
- Protect VeloCloud Orchestrator administrative credentials and management access.
- Obtain and distribute VeloCloud Edge software only through trusted Arista management and distribution channels.
- Investigate unexpected software images or update operations before permitting installation.

These measures reduce exposure but do not correct the vulnerable update-verification workflow.

Resolution

Migrating to a patched software version for VeloCloud Edge is the advised course of action.

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.

Arista suggests that operators transition to the most recent release within a supported branch that incorporates the necessary remediations.

The vulnerability identified as CVE-2026-86109 is addressed in the following versions:

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

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

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.