Date: May 8, 2026

Revision	Date	Changes
1.0	May 8, 2026	Initial release

The CVE-ID's tracking this issue: CVE-2026-43284, and CVE-2026-43500.

Description

Arista Networks is providing this security update in response to a recent, publicly disclosed security vulnerability widely known as "Dirty Frag". Exploitation of this issue allows for an unprivileged local user to gain root access to a device by running an executable binary. Access to an environment where arbitrary code can be executed is required for this vulnerability to be exploitable.

This issue was reported externally. The external researchers website for this issue is https://github.com/V4bel/dirtyfrag.

Vulnerability Assessment

Affected Software

There is no Arista software known to be affected as of this advisory being posted.

Affected Platforms

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

- There are no Arista platforms known to be affected as of this advisory being posted.

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 7130 Systems running MOS
- 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
- Arista Converged Cloud Fabric (formerly Big Switch BCF)
- Arista DANZ Monitoring Fabric (formerly Big Switch BMF)
- CloudVision AGNI - Cloud service delivery
- Arista Edge Threat Management - Arista NG Firewall and Arista Micro Edge (Formerly Untangle)

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

- Arista Network Detection and Response (NDR) Security Platform (Formerly Awake NDR)
- 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)
- VeloCloud Edge (Formerly VeloCloud Edge by Broadcom)
- CloudVision AGNI - Virtual or physical appliance

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