Date: May 8, 2026

Revision	Date	Changes
1.0	May 8, 2026	Initial release
1.1	May 18, 2026	Updated affected products and added Mitigation section
1.2	July 15, 2026	Updated CVE-ID's tracking this issue Updated Affected Software Added Resolution section

The CVE-ID’s tracking this issue: CVE-2026-43284, CVE-2026-43500, and CVE-2026-43503.

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

- VeloCloud Orchestrator (Formerly VeloCloud Orchestrator by Broadcom)
    - Release 6.4.2.0 and below
    - Release 6.1.3.1 and below
    - Release 5.2.3.11 and below
- VeloCloud Gateway (Formerly VeloCloud Gateway by Broadcom)
    - Release 6.4.2.0 (GA builds before R6420-20260629-GA-90d3261d11-228)
    - Release 6.2.0.1
    - Release 6.1.2.2 and below
    - Release 5.2.6 and below

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)
- VeloCloud Gateway (Formerly VeloCloud Gateway 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 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

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 Edge Threat Management - Arista NG Firewall and Arista Micro Edge (Formerly Untangle)
- Arista Network Detection and Response (NDR) Security Platform (Formerly Awake NDR)
- VeloCloud Edge (Formerly VeloCloud Edge by Broadcom)
- CloudVision AGNI - Virtual or physical appliance

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

- Arista NetVisor OS, Arista NetVisor UNUM, and Insight Analytics (Formerly Pluribus)

Mitigation

Velocloud Gateway and Orchestrator

This issue can be mitigated on the Velocloud Gateway and Orchestrator without a software upgrade by blocking the esp4, esp6 and rxrpc kernel module from loading. This prevents the exploit from reaching the vulnerable code path while leaving all other VCG/VCO functions (IPsec, TLS, encryption) unaffected.

```
# Step 1: Check current module status (before)
# Note the output. The module may or may not be loaded.
$ lsmod | grep esp4
$ lsmod | grep esp6
$ lsmod | grep rxrpc

# Step 2: Block the module
$ echo "install esp4 /bin/false" >> /etc/modprobe.d/cis.conf
$ echo "install esp6 /bin/false" >> /etc/modprobe.d/cis.conf
$ echo "install rxrpc /bin/false" >> /etc/modprobe.d/cis.conf

# Step 3: Unload the module if currently loaded
$ rmmod esp4 2>/dev/null
$ rmmod esp6 2>/dev/null
$ rmmod rxrpc 2>/dev/null

# Step 4: Verify the mitigation
# Expected output: empty (no output). The module is not loaded.
$ lsmod | grep esp4
$ lsmod | grep esp6
$ lsmod | grep rxrpc

# Step 5: Confirm the block is in the configuration:
```

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.

```
# Expected output: install esp4 /bin/false
# Expected output: install esp6 /bin/false
# Expected output: install rxrpc /bin/false
$ grep esp4 /etc/modprobe.d/cis.conf
$ grep esp6 /etc/modprobe.d/cis.conf
$ grep rxrpc /etc/modprobe.d/cis.conf

# Step 6: Confirm the module cannot be loaded:
# Expected output: modprobe: ERROR: could not insert
# 'esp4':= Invalid argument'
# 'esp6':= Invalid argument'
# 'rxrpc':= Invalid argument'

$ modprobe esp4
$ modprobe esp6
$ modprobe rxrpc

# Step 7: verify in a second location. Expected output: empty (no output)
$ lsmod | grep esp4
$ lsmod | grep esp6
$ lsmod | grep rxrpc

# If the module did load, manually remove the
# module by doing `modprobe -r esp4`, `modprobe -r esp6`, `modprobe -r rxrpc` and res
tart from Step 1
```

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.

- VeloCloud Orchestrator (Formerly VeloCloud Orchestrator by Broadcom)
    - Release 6.4.2.1
    - Release 6.1.3.2
    - Release 5.2.3.12
    -
- VeloCloud Gateway (Formerly VeloCloud Gateway by Broadcom)
    - Release 7.0.0.0
    - Release 6.4.2.0 (R6420-20260629-GA-90d3261d11-228)
    - Release 6.1.4.0
    - Release 5.2.7.0 (next release)

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.

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.