Date: August 19, 2026

Revision	Date	Changes
1.0	August 19, 2026	Initial release

Description

Arista Networks is providing this security update in response to the following list of gRPC-go security vulnerabilities posted by Google at https://github.com/advisories/GHSA-hrxh-6v49-42gf. Arista EOS-based products and WI-FI Access Point incorporate the affected gRPC-go framework.

Arista products are affected solely by the HTTP/2 Rapid Reset DOS Bypass vulnerability, wherein an unauthenticated remote attacker can exploit unthrottled HTTP/2 stream reset to bypass rate-limiting controls, consuming excessive CPU resources and causing a Denial of Service (DoS). Arista products are not impacted by the xDS RBAC vulnerabilities.

This issue is tracked internally by BUG1866958(EOS), BUG1870148(EOS), BUG1870119(WIFI AP).

For comprehensive technical details regarding the gRPC-go vulnerabilities, encompassing affected components and CVSS severity ratings, please consult the upstream security advisory referenced above.

Currently, the remediated software releases are under development and in the process of being shipped across the various affected release trains. Arista will continue to update this advisory as soon as the respective releases containing the official fix have been published.

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

EOS Versions

- 4.36.1F and below releases in the 4.36 train
- 4.35.5M and below releases in the 4.35 train
- 4.34.7.1M and below releases in the 4.34 train

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.

- 4.33.8M and below releases in the 4.33 train
- All prior releases

Streaming Telemetry Agent Version

- v1.45.0
- v1.43.7 and below releases in the v1.43 train
- All releases in the v1.42 train
- All releases in the v1.41 train
- v1.40.12 and below releases in the v1.40 train
- All releases in the v1.39 train
- All releases in the v1.38 train
- v1.37.12 and below releases in the v1.37 train
- All releases in the v1.36 train
- All releases in the v1.35 train
- v1.34.13 and below releases in the v1.34 train
- All releases in the v1.33 train
- All releases in the v1.32 train
- v1.31.16 and below releases in the v1.31 train
- All releases in all trains prior to v1.31

WI-FI Access Points

- 21.3.0M-13 and below releases in the 21.x train
- All prior releases

Affected Platforms

The following products **are** affected by HTTP/2 Rapid Reset DOS Bypass:

- 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

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.

    - 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
- WI-FI Access Points

The following products are **NOT** affected:

- 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)
- VeloCloud Gateway (Formerly VeloCloud Gateway by Broadcom)
- VeloCloud Edge (Formerly VeloCloud Edge by Broadcom)

Required Configuration for Exploitation

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 EOS-based products

In order to be vulnerable to HTTP/2 Rapid Reset DOS Bypass vulnerability, **any** of the following non-default configurations must be present, which enables a gRPC server:

gNMI

OpenConfig gNMI is enabled on the device:

```
switch# show running-config section gnmi
management api gnmi
   transport grpc <TRANSPORT_NAME>
```

gRIBI

gRPC Routing Information Base Interface (gRIBI) is enabled on the device:

```
switch# show running-config section gribi
management api gribi
   transport grpc <TRANSPORT_NAME>
```

Streaming Telemetry Agent

Streaming Telemetry Agent is enabled on the device with gRPC server configured:

```
switch# show running-config section grpcaddr
daemon TerminAttr
   exec /usr/bin/TerminAttr -grpcaddr <GRPC_ADDR>
```

WI-FI Access Points

WIFI Access Points are affected by HTTP/2 Rapid Reset DOS Bypass vulnerability when AP is operating in OpenConfig mode. To check if AP is in openconfig mode, run the following CLI command from the AP config shell.

```
[config]$ show openconfig
Operating mode: openconfig
This mode supports SET, GET and STREAM via GNMI.
```

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.

Indicators of Compromise

For the HTTP/2 Rapid Reset bypass vulnerability, monitor for anomalous spikes in CPU utilization that do not align with application traffic volume. Inspect network or proxy logs for an unusually high ratio of client-initiated HEADERS frames followed immediately by RST_STREAM frames on a single connection.

Arista EOS-based products

The following procedures can be used to determine whether a device is experiencing anomalous CPU utilization that may indicate exploitation of this vulnerability.

gNMI

For devices running OpenConfig or Octa agent for gNMI transport:

```
switch# show agent OpenConfig cpu
switch# show agent Octa cpu
```

gRIBI

For devices running Gribi agent for gRIBI transport:

```
switch# show agent Gribi cpu
```

Streaming Telemetry Agent

For devices running the TerminAttr daemon, use the show process top command to identify processes consuming excessive CPU:

```
switch# show process top memory
```

In the output, locate the TerminAttr process. Under normal operating conditions, TerminAttr CPU usage should be consistent with the volume of streaming telemetry subscriptions and CloudVision interactions configured on the device. Unexplained, sustained spikes in TerminAttr CPU consumption may indicate exploitation.

Mitigation

Arista EOS-based products

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.

Enforcing Mutual TLS (mTLS) can largely reduce the risk of exploitation of HTTP/2 Rapid Reset DOS Bypass vulnerability by increasing the difficulty for exploitation from an unauthenticated remote vector to authenticated users only.

First create an SSL profile using the certificate. For more details on certificate generation and EOS-based product SSL profile management, please refer to the article Working with certificates.

For example, the following OpenConfig gRPC server is configured with mTLS:

```
management security
   ssl profile mtls-grpc-profile
      certificate target.crt key target.key
      trust certificate ca.crt
```

For gNMI:

```
management api gnmi
   transport grpc default
      ssl profile mtls-grpc-profile
```

For gRIBI:

```
management api gribi
   transport grpc default
      ssl profile mtls-grpc-profile
```

For Streaming Telemetry Agent, specify the certificate and key file used by gRPC server

```
daemon TerminAttr
   exec /usr/bin/TerminAttr -grpcaddr <GRPC_ADDR>
      -certfile /persist/secure/ssl/certs/target.crt
      -keyfile /persist/secure/ssl/keys/target.key
      -clientcafile /persist/secure/ssl/certs/ca.crt
   no shutdown
```

WI-FI Access Points

There is no mitigation available to address HTTP/2 Rapid Reset DOS Bypass 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.

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.

HTTP/2 Rapid Reset DOS Bypass vulnerability has been fixed in the following product releases. As new releases are provided this page will be updated:

Arista EOS-based products

- 4.36.2F and later releases in the 4.36 train
- 4.35.6M and later releases in the 4.35 train
- 4.34.8M and later releases in the 4.34 train
- 4.33.9M and later releases in the 4.33 train

For more information about upgrading EOS releases, see EOS User Manual: Upgrades and Downgrades

Streaming Telemetry Agent Version

- v1.46.0 and all later releases
- v1.45.1
- v1.43.8 and later releases in the v1.43 train
- v1.40.13 and later releases in the v1.40 train
- v1.37.13 and later releases in the v1.37 train
- v1.34.14 and later releases in the v1.34 train
- v1.31.17 and later releases in the v1.31 train

For more information about upgrading Streaming Telemetry Agent release versions on EOS switch, see TerminAttr – Upgrade & Downgrade.

Note: fully mitigating the vulnerability across all affected services, including gNMI and gRIBI, requires a complete EOS image upgrade. Upgrading the Streaming Telemetry Agent alone addresses the vulnerability for telemetry streams only.

WI-FI Access Points

- 21.4.0M-12 and later releases in the 21.x train

Hotfix

No hotfix is available for this issue.

For More Information

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.

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.