Date: September 9, 2026

Revision	Date	Changes
1.0	September 9, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-73458
CVSSv3.1 Base Score: 8.2 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H)
CVSSv4.0 Base Score: 9.2
(CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:H/SC:N/SI:N/SA:H)
Common Weakness Enumeration: CWE-303: Incorrect Implementation of Authentication Algorithm
This vulnerability is being tracked by BUG 1787150

Description

On affected platforms running Arista EOS with authenticated Bidirectional Forwarding Detection (BFD) sessions configured, a specially crafted packet can cause the BFD session(s) to go down. This may result in undesirable network changes because various routing protocols monitor status on BFD session(s).

This issue was discovered internally by Arista, and the company 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.x train
- 4.35.5M and below releases in the 4.35.x train
- 4.34.7M and below releases in the 4.34.x train
- 4.33.8M and below releases in the 4.33.x train
- All prior releases

Affected Platforms

The following products **are** 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

The following product versions and platforms **are not** affected by this vulnerability:

- 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
- 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 DANZ Monitoring Fabric (formerly Big Switch BMF)
- 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

In order to be vulnerable to CVE-2026-73458, the following condition must be met:

BFD sessions configured with authentication are affected by this issue. All supported authentication modes are impacted. The full list of authentication modes is below:

- Password
- Keyed MD5
- Meticulous MD5
- Keyed SHA1
- Meticulous SHA1

To determine whether your sessions are affected, run the following show command. If the authentication mode is set to anything other than None, your configuration is impacted. In the example below, the authentication mode is set to Password, indicating an affected configuration.

```
switch>show bfd peers detail
VRF name: default
-----------------
Peer Addr 1.0.0.2, Intf Ethernet3/30/3, Type normal, Role active, State Up
VRF default, LAddr 1.0.0.1, LD/RD 2432996710/3471785639
Session state is Up and not using echo function
Hardware Acceleration: Async Off, Echo Off
Last Up 06/04/26 13:55:50.630
Last Down 06/04/26 13:55:49.725
Last Diag: No Diagnostic
Authentication mode: Password
Shared-secret profile: bfdProfile_0
TxInt: 500 ms, RxInt: 500 ms, Multiplier: 20
Received RxInt: 500 ms, Received Multiplier: 20
Rx Count: 2308, Rx Interval (ms) min/max/avg: 81/538/438 last: 188 ms ago
Tx Count: 2206, Tx Interval (ms) min/max/avg: 380/516/458 last: 476 ms ago
Detect Time: 10000 ms
Sched Delay: 1*TxInt: 1762, 2*TxInt: 443, 3*TxInt: 0, GT 3*TxInt: 0
Registered protocols: bgp
```

```
Uptime: 16:51.08
Last packet:  Version: 1              - Diagnostic: 0
              State bit: Up           - Demand bit: 0
              Poll bit: 0             - Final bit: 0
              Multiplier: 20          - Length: 38
              My Discr.: 3471785639   - Your Discr.: 2432996710
              Min tx interval: 500    - Min rx interval: 500
              Min Echo interval: 500
```

If BFD is not configured, there is no exposure to this issue. The below show command command will return empty output:

```
switch>show running-config section bfd
switch>
```

If BFD is configured but not operational, there is no exposure to this issue. The below show command will return empty output:

```
switch>show bfd peers detail
switch>
```

If BFD is configured, and operational but not in authentication mode, there is no exposure to this issue and the output of below show command will look something like:

```
switch>show bfd peers detail
VRF name: default
-----------------
Peer Addr 1.0.0.2, Intf Ethernet3/30/3, Type normal, Role active, State Up
VRF default, LAddr 1.0.0.1, LD/RD 2432996710/3471785639
Session state is Up and not using echo function
Hardware Acceleration: Async On, Echo Off
Last Up 06/04/26 14:15:32.259
Last Down 06/04/26 14:14:50.328
Last Diag: No Diagnostic
Authentication mode: None
Shared-secret profile: None
TxInt: 500 ms, RxInt: 500 ms, Multiplier: 20
Received RxInt: 500 ms, Received Multiplier: 20
Rx Count: 34, Rx Interval (ms) min/max/avg: 161/496/408 last: 163 ms ago
Tx Count: 29, Tx Interval (ms) min/max/avg: 375/499/440 last: 720 ms ago
```

```
Detect Time: 10000 ms
Sched Delay: 1*TxInt: 76, 2*TxInt: 0, 3*TxInt: 0, GT 3*TxInt: 0
Registered protocols: bgp
Uptime: 13.65
Last packet:  Version: 1              - Diagnostic: 0
              State bit: Up           - Demand bit: 0
              Poll bit: 0             - Final bit: 0
              Multiplier: 20          - Length: 24
              My Discr.: 3471785639   - Your Discr.: 2432996710
              Min tx interval: 500    - Min rx interval: 500
              Min Echo interval: 500
```

Indicators of Compromise

No indicators of compromise are available for this issue.

Mitigation

No mitigation is 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. For more information about upgrading see EOS User Manual: Upgrades and Downgrades

CVE-2026-73458 has been fixed in the following releases:

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

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