Date: November 10, 2026

Revision	Date	Changes
1.0	November 10, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-121368
CVSSv3.1 Base Score: 8.6 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H)
CVSSv4.0 Base Score: 8.9
(CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:H)
Common Weakness Enumeration: CWE-787: Out-of-bounds Write.
This vulnerability is being tracked by BUG 1965007

Description

On affected platforms running Arista EOS with Bidirectional Forwarding Detection (BFD) configured to use keyed MD5 or keyed SHA1 authentication, an unauthenticated attacker with network adjacency (direct or multi-hop) to a BFD-enabled interface can send a specially crafted BFD packet resulting in a system reboot.

This issue was discovered externally by Joshua Foote from the XOR team at JP Morgan Chase & Co. and Arista is not aware of any malicious uses of this issue 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

- 4.36.2F and below releases in the 4.36.x train
- 4.35.6M and below releases in the 4.35.x train
- 4.34.8M and below releases in the 4.34.x train
- 4.33.10M and below releases in the 4.33.x train
- All releases in the 4.32.x train
- All releases in the End of Support software release trains back to and including 4.22.0

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.

- 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/XE7 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
  - ZTX-7200 Series
  - CloudEOS
  - cEOS-lab
  - vEOS-lab
  - CloudVision eXchange, virtual or physical appliance

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

- Wi-Fi Access Points
- CloudVision CUE cloud service delivery
- CloudVision Portal on-premises, virtual appliance or physical appliance (including the CV-CUE on-premises software)
- 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)

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 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

In order to be vulnerable to CVE-2026-121368, the following condition must be met:

BFD authentication must be configured for either MD5 or SHA1 hashing. Either authentication scheme may optionally be configured to run in meticulous mode.

To check whether the device is affected, inspect the running configuration with the following show command:

Any of the following configurations in use with live BFD sessions indicate the device is vulnerable:

```
switch(s1)#show running-config section router bfd
router bfd
   authentication mode md5 shared-secret profile profile1
```

```
switch(s1)#show running-config section router bfd
router bfd
   authentication mode md5 shared-secret profile profile1 meticulous
```

```
switch(s1)#show running-config section router bfd
router bfd
   authentication mode sha1 shared-secret profile profile1
```

```
switch(s1)#show running-config section router bfd
router bfd
   authentication mode sha1 shared-secret profile profile1 meticulous
```

If neither MD5 nor SHA1 authentication for BFD sessions are enabled, the above configurations

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.

will be missing from the output of “show running-config”.

Note that the same configuration item indicating BFD session authentication may also appear under the device’s per-interface configuration.

```
switch(s1)#show running-config section bfd
interface Ethernet1
   bfd authentication mode md5 shared-secret profile profile1
```

Session authentication configured per-interface takes precedence over device-wide authentication configuration. If all BFD sessions on a device have per-interface authentication configuration overriding global authentication then exposure is dependent on the per-interface configuration only, while it is in place

The following show-command output indicates the authentication mode of each session:

```
switch(s1)#show bfd peers detail
VRF name: default
-----------------
Peer Addr 2001:db8::2, Intf Ethernet1, Type normal, Role active, State Up
VRF default, LAddr 2001:db8::1, LD/RD 12345/67890
Session state is Up and not using echo function
Hardware Acceleration: Async Off, Echo Off
Last Up 11/04/26 10:00:00.123
Last Down NA
Last Diag: No Diagnostic
Authentication mode: Keyed Sha1
Shared-secret profile: BFD_KEYS
TxInt: 300 ms, RxInt: 300 ms, Multiplier: 3
Received RxInt: 300 ms, Received Multiplier: 3
Rx Count: 13716, Rx Interval (ms) min/max/avg: 225/301/262 last: 104 ms ago
Tx Count: 13719, Tx Interval (ms) min/max/avg: 0/2/0 last: 87 ms ago
Detect Time: 900 ms
Sched Delay: 1*TxInt: 13719, 2*TxInt: 0, 3*TxInt: 0, GT 3*TxInt: 0
Registered protocols: bgp
Uptime: 01:00:00.00
Last packet: Version: 1              - Diagnostic: 0
             State bit: Up          - Demand bit: 0
             Poll bit: 0            - Final bit: 0
             Multiplier: 3          - Length: 52
             My Discr.: 67890       - Your Discr.: 12345
             Min tx interval: 300   - Min rx interval: 300
             Min Echo interval: 0
```

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.

Authentication modes which may be shown in the above show-command output and indicate exposure include:

- “Keyed Sha1”
- “Keyed Md5”
- “Meticulous Sha1”
- “Meticulous Md5”

Indicators of Compromise

This vulnerability may lead to kernel-panic and unexpected reboot of the affected device.

The following kernel messages may also appear which indicate the issue:

```
rbfd Rx: Packet failed RFC validation due to 4
rbfd Rx (1234): Packet failed auth check

rbfd Rx (1234): key id not found 7
rbfd Rx (1234): seqnum failed received 100 expected >= 101
rbfd Rx (1234): seqnum failed received 100 expected > 101 and <= 102
rbfd Rx (1234): auth ifindex 12 skb ifindex 15
```

In all above examples, all reason code, discriminator, key ID, sequence number, and ifIndex values are subject to change depending on the customer configuration and BFD session state at the time of logging.

The above messages may appear in “/var/log/messages” if the device is running an EOS version prior to the 4.30.0F. All subsequent releases write rbfd logging to “/var/log/rbfd.log”.

In order for these logs to appear, configuration for elevated rbfd logging (level 2 or greater) must be present on the device, logging level can be checked with the below show command.

```
switch(s1)#show running-config section router bfd
router bfd
   debug rbfd 2
```

Mitigation

No mitigation is available for this issue.

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. For more information about upgrading see EOS Manual: Upgrades and Downgrades.

CVE-2026-121368 has been fixed in the following releases:

- 4.37.0F and later releases in the 4.37.x train
- 4.36.3M and later releases in the 4.36.x train
- 4.35.7M and later releases in the 4.35.x train
- 4.34.9M and later releases in the 4.34.x train
- 4.33.11M 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
- By email: support@arista.com
- By telephone: List of regional telephone numbers

Receive notification for new advisories and notices:

Subscribe to the RSS feed and email notifications to receive periodic updates on new software releases, advisories, end of sale and field notices.

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.