Date: September 9, 2026

Revision	Date	Changes
1.0	September 9, 2026	Initial release

Description

All of the CVEs covered in this advisory apply to affected platforms running Arista EOS with Intermediate System to Intermediate System (IS-IS) configured. In all three cases, an unauthenticated attacker in the same Layer 2 domain as the target device can manipulate IS-IS protocol state, potentially bypassing the protections offered by RFC 5304/5310 MD5 or SHA authentication.

All of these issues were discovered internally by Arista and the company is not aware of any malicious uses of these issues in customer networks.

CVE-2026-73446

On affected platforms running Arista EOS with IS-IS configured on a broadcast interface, an unauthenticated attacker can send a crafted IS-IS Hello Protocol Data Unit (PDU) that causes the device to tear down an established IS-IS adjacency. This may result in traffic disruption and loss of IP reachability for prefixes advertised through that adjacency.

CVSSv3.1 Base Score: 7.4 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H)
CVSSv4.0 Base Score: 7
(CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:H)
Common Weakness Enumeration: CWE-696: Incorrect Behavior Order This vulnerability is being tracked by BUG1840504

CVE-2026-73459

On affected platforms running Arista EOS with IS-IS configured, an unauthenticated attacker who can inject a specially crafted IS-IS LSP PDU can cause the legitimate LSP to be unexpectedly purged from the IS-IS link-state database. This may result in traffic loss.

CVSSv3.1 Base Score: 7.4 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H)
CVSSv4.0 Base Score: 7
(CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:H)
Common Weakness Enumeration: CWE-354: Improper Validation of Integrity Check Value
This vulnerability is being tracked by BUG1840507

CVE-2026-73460

On affected platforms running Arista EOS with IS-IS graceful restart enabled, an unauthenticated attacker who can inject a malformed IS-IS LSP PDU packet can cause the IS-

IS graceful restart procedure to terminate prematurely. This may result in traffic loss following a restart event.

CVSSv3.1 Base Score: 6.1 (CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:H)
CVSSv4.0 Base Score: 7
(CVSS:4.0/AV:A/AC:H/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:H)
Common Weakness Enumeration: CWE-863: Incorrect Authorization
This vulnerability is being tracked by BUG1840562

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

CVE-2026-73446

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
- 4.34.7.1M and below releases in the 4.34.x train
- 4.33.9M and below releases in the 4.33.x train
- All releases in 4.32.x and 4.31.x trains

CVE-2026-73459

EOS Versions

- 4.36.1F and below releases in the 4.36.x train

CVE-2026-73460

EOS Versions

- 4.36.1F and below releases in the 4.36.x train

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:

- WI-FI 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
- 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

CVE-2026-73446

In order to be vulnerable to CVE-2026-73446, the following condition must be met:

IS-IS must be enabled on a broadcast (LAN) interface AND there should be an active IS-IS adjacency on that interface:

```
switch(config-router-isis)#show active
router isis 1
   net 49.0001.1111.1111.1001.00
switch(config-if-Et1)#show active
interface Ethernet1
   isis enable 1
```

```
switch#show isis interface detail
IS-IS Instance: 1 VRF: default

  Interface Ethernet1:
    Index: 4 SNPA: 2:2:0:1:0:0
    MTU: 1497 Type: broadcast
    Supported address families: IPv4, IPv6
    Area proxy boundary is disabled
    BFD IPv4 is disabled
    BFD IPv6 is disabled
    Hello padding is enabled
    Level 1:
      Metric: 10, Number of adjacencies: 1
      LAN-ID: 1111.1111.1001.04, Priority: 64
      DIS: 1111.1111.1001, DIS priority: 64
      Authentication mode: None
      TI-LFA protection is disabled for IPv4
      TI-LFA protection is disabled for IPv6
    Adjacency 1111.1111.1002:
```

```
    State: UP, Level: 1 Type: Level 1 IS
    Advertised hold time: 9
    Neighbor supported address families: IPv4, IPv6
    Address family match: Enabled
    SNPA: 2:2:0:2:0:0, Priority: 64
    IPv4 interface address: 10.0.0.2
    IPv6 interface address: fe80::2:ff:fe02:0
    Area addresses: 49.0001
```

If IS-IS is not configured OR IS-IS is configured only on point-to-point interfaces, there is no exposure to this issue.

```
switch#show isis interface detail
IS-IS Instance: 1 VRF: default

 Interface Ethernet1:
   Index: 4 SNPA: P2P
   MTU: 1497 Type: point-to-point
   Supported address families: IPv4, IPv6
   Area proxy boundary is disabled
   BFD IPv4 is disabled
   BFD IPv6 is disabled
   Hello padding is enabled
   Local fast flooding is disabled
   Level 1:
     Metric: 10, Number of adjacencies: 1
     Link-ID: 04
     Authentication mode: None
     TI-LFA protection is disabled for IPv4
     TI-LFA protection is disabled for IPv6
   Adjacency 1111.1111.1002:
     State: UP, Level: 1 Type: Level 1 IS
     Advertised hold time: 30
     Neighbor supported address families: IPv4, IPv6
     Address family match: Enabled
     IPv4 interface address: 1.0.0.2
     IPv6 interface address: fe80::2:ff:fe02:0
     Area addresses: 49.0001
     Peer fast flooding is disabled
```

CVE-2026-73459

In order to be vulnerable to CVE-2026-73459, the following condition must be met:

IS-IS should be configured.

```
switch# show isis summary
IS-IS Instance: 1 VRF: default
  Instance ID: 0
  System ID: 1111.1111.1001, administratively enabled
  Router ID: IPv4: 0.0.0.0
  Multi Topology disabled, not attached
  IPv4 Preference: Level 1: 115, Level 2: 115
  IPv6 Preference: Level 1: 115, Level 2: 115
  IS-Type: Level 1 and 2, Number active interfaces: 1
  Routes both IPv4 and IPv6
  LSP size maximum: Level 1: 1492, Level 2: 1492
  Interval Type           Max Wait Initial Wait Hold Interval
  ----------------------- -------- ------------ -------------
  LSP generation interval      5 s        50 ms         50 ms
  SPF interval             30000 ms       300 ms         80 ms
  Current SPF hold interval(ms): Level 1: 80, Level 2: 80
  Last Level 1 SPF run 9 seconds ago
  Last Level 2 SPF run 9 seconds ago
  CSNP generation interval: 10 seconds
  Dynamic Flooding: Disabled
  Authentication mode: Level 1: None, Level 2: None
  Graceful Restart: Disabled, Graceful Restart Helper: Enabled
  Area addresses: 40
  level 1: number DIS interfaces: 0, LSDB size: 1
    Area Leader: None
    Overload Bit is not set.
  level 2: number DIS interfaces: 0, LSDB size: 1
    Area Leader: None
    Overload Bit is not set.
  Redistributed Level 1 routes: 0 limit: Not Configured
  Redistributed Level 2 routes: 0 limit: Not Configured
```

If IS-IS is not configured, there is no exposure to this issue.

```
switch#show isis summary
switch#
```

CVE-2026-73460

In order to be vulnerable to CVE-2026-73460, the following condition must be met:

IS-IS graceful-restart should be enabled.

```
switch(config-router-isis)#show active
router isis 1
   net 49.0001.1111.1111.1001.00
   graceful-restart
```

```
switch#show isis graceful-restart
IS-IS Instance: 1 VRF: default
  System ID: 1111.1111.1001
  Graceful Restart: Enabled, Graceful Restart Helper: Enabled
  State: Graceful Restart disabled during startup
  T1 : 3s
  T2 (level-1) : 30s/not running
  T2 (level-2) : 30s/not running
  T3 : not running
  System ID          Type    Interface          Restart Capable   Status
  1111.1111.1002     L1      Ethernet1          Yes               Running
```

If IS-IS graceful-restart is not enabled, there is no exposure to this issue.

Indicators of Compromise

CVE-2026-73446

This vulnerability may lead to deletion of the established IS-IS adjacency on a broadcast interface. The following syslog message may appear:

```
10:10:11.401817 Instance 0: %ISIS-4-ISIS_ADJCHG: L1 Neighbor State Change for 1111.11
11.1002 on Et1 to DOWN: hold timer expired
```

CVE-2026-73459

This vulnerability may lead to the unintended removal of LSPs originated by self or another router in the network.
An increase in the drop counter may be observed.

```
switch# show isis counters drop details
```

```
IS-IS Instance: 1 VRF: default
Drop Details
------------

Ethernet1
---------
LSP L2:
-------
Drop Reason                  Drop Count
Different Checksum Lsp               1
```

Additionally, a log in **show isis lsp purges** is indicative of an LSP being dropped due to a checksum mismatch.

```
switch# show isis lsp purges
IS-IS Instance: 1 VRF: default
IS-IS Level-2
2026-08-20 12:34:56.123456 Purge of 0000.0003.0036.00-00 generated by self, LSP has a
 different checksum             1
```

CVE-2026-73460

An indicator of this issue is an IS-IS syslog message reporting a malformed or unauthenticated packet during a graceful restart, followed by traffic disruption.

The presence of one of the following log messages indicates potential exploitation:

```
ISIS-3-ISIS_LSP_CORRUPT: L[12] LSP ID: ., Intf., Sequence number .*
ISIS-3-ISIS_LSP_IGNORED: L[12] LSP ID: ., ' \
                           'Sequence number .* Failed to authenticate'
```

Mitigation

CVE-2026-73446

The workaround is to configure the IS-IS interface type as point-to-point instead of the default broadcast (LAN). This must be done on both endpoints of the link.

```
switch(config-if-Et1)#show active
interface Ethernet1
   isis enable 1
```

```
isis network point-to-point
```

Changing the IS-IS interface type from LAN to point-to-point may result in temporary adjacency flaps on the specified link, potentially causing transient traffic loss.

The above mitigation does not work in cases where the LAN interface supports multiple IS-IS adjacencies. In such instances, the peerings must be partitioned across separate point-to-point interfaces to ensure each interface maps to a single IS-IS adjacency.

CVE-2026-73459 and CVE-2026-73460

No workaround is available for those issues.

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-2026-73446 (BUG1840504) 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
- 4.33.10M and later releases in the 4.33.x train

CVE-2026-73459 (BUG1840507) has been fixed in the following releases:

- 4.36.2F and later releases in the 4.36.x train

CVE-2026-73460 (BUG1840562) has been fixed in the following releases:

- 4.36.2F and later releases in the 4.36.x train

Hotfix

There is no hotfix 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