Date: September 9, 2026

Revision	Date	Changes
1.0	September 9, 2026	Initial release
1.1	September 22, 2026	CSAF JSON file added

The CVE-ID tracking this issue: CVE-2026-73450
CVSSv3.1 Base Score: 6.9 (CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:H)
CVSSv4.0 Base Score: 7
(CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:N/VI:L/VA:H/SC:N/SI:N/SA:H)
Common Weakness Enumeration: CWE-345: Insufficient Verification of Data Authenticity
This vulnerability is being tracked by BUG1852792

Description

On affected platforms running Arista EOS with MLAG Dual Primary Detection configured, an unauthenticated attacker with access to the Dual Primary Detection network segment can send specially crafted packets to interfere with the dual-primary state. If the MLAG primary switch fails while these packets are present, the secondary switch incorrectly concludes it is in a dual-primary condition and err-disables its interfaces, leading to a traffic interruption.

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
- 4.34.7.1M and below releases in the 4.34.x train
- 4.33.9M and below releases in the 4.33.x train
- All prior releases

Affected Platforms

- 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 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-2026-73450, all of the following conditions must be met:

1. MLAG must be configured
2. domain-id and peer-link are active
3. UDP heartbeat peer address must be configured
4. dual-primary detection must be configured with action **errdisable all-interfaces**

Both peers must have this configuration applied to be vulnerable.

Example vulnerable configuration:

```
switch(config)# mlag
switch(config-mlag)# peer-link port-channel 10
switch(config-mlag)# domain-id mlagDomain
switch(config-mlag)# peer-address heartbeat 172.30.118.190
switch(config-mlag)# dual-primary detection delay 5 action errdisable all-interfaces
```

Example show command output for vulnerable configuration:

```
switch# show mlag
MLAG Configuration:
domain-id          :         mlagDomain
local-interface    :           Vlan4094
peer-address       :           10.0.0.2
peer-link          :     Port-Channel10
hb-peer-address    :     172.30.118.190

MLAG Status:
state              :             Active
…
MLAG ports:
…

MLAG Detailed Status:
```

```
…
Dual-primary detection delay         :                   5
Dual-primary action                  :      errdisable-all
Dual-primary recovery delay          :                   0
Dual-primary non-mlag recovery delay :                   0
```

Indicators of Compromise

If this vulnerability is exploited, the secondary switch in the MLAG pair will have its interfaces placed into an errdisabled state. Key indicators include the secondary MLAG peer transitioning to a dual-primary detected state with its interfaces errdisabled, while the primary peer remains inactive (whether shut down, rebooted, or unreachable).

The following may be present to show that secondary peer entered into dual-primary detected state:

```
switch(config)#show Mlag detail
…
MLAG Status:
...
Peer-link status               : Down
Dual-primary detection         : Detected
dual-primary interface errdisabled : True
UDP heartbeat alive             : True
…

switch(config)#show interfaces status errdisabled
Port      Status        Reason
--------- ------------- ------------------
Et1       errdisabled   mlagdualprimary
Et2       errdisabled   mlagdualprimary
Et14      errdisabled   mlagdualprimary
…
```

The following may be present to show that primary peer is inactive:

```
switch(config)#show Mlag detail
…
MLAG Status:
state             :             Inactive
…
```

The following message may appear in Syslog messages for MLAG agent:

```
%MLAG-4-DUAL_PRIMARY: MLAG dual-primary condition is detected
```

Mitigation

Restrict access to the MLAG heartbeat interface by configuring Access Control Lists (ACLs) to permit traffic strictly from the designated peer address.

Insert the following ACL rules into the top of the ingress ACL on the VRF where the heartbeat address is configured, while denying traffic from all other source addresses.

```
permit udp host <heartbeatPeerAddress> any eq mlag
permit udp any any eq mlag ttl eq 255
deny udp any any eq mlag log
```

Ensure administrative access for required services (e.g., SSH, NTP, SNMP) remains permitted.

For detailed instructions on configuring custom control plane ACLs, refer to the Default Control-plane ACL Override.

For instance, if the heartbeat address is reachable via the management VRF. First, construct the ingress ACL to restrict access on the MLAG heartbeat interface.

```
switch(config)#ip access-list MLAG-HEARTBEAT-PROTECT
switch(config-acl-MLAG-HEARTBEAT-
PROTECT)#5 permit udp host 172.30.118.190 any eq mlag
switch(config-acl-MLAG-HEARTBEAT-PROTECT)#6 permit udp any any eq mlag ttl eq 255
switch(config-acl-MLAG-HEARTBEAT-PROTECT)#7 deny udp any any eq mlag log
...
```

Apply the ACL to management VRF:

```
switch(config)#system control-plane
switch(config-system-cp)#ip access-group MLAG-HEARTBEAT-PROTECT vrf management in
switch(config-system-cp)#exit
```

Show command to confirm the rules:

```
switch(config)#show ip access-lists MLAG-HEARTBEAT-PROTECT
Phone ACL bypass: disabled
IP Access List MLAG-HEARTBEAT-PROTECT
        5 permit udp host 172.30.118.190 any eq mlag
        6 permit udp any any eq mlag ttl eq 255
        7 deny udp any any eq mlag log
        …

        Total rules configured: …
        Configured on Ingress: control-plane(management VRF)
        Active on     Ingress: control-plane(management VRF)
```

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-2026-73450 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

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