Date: January 24, 2025

Revision	Date	Changes
1.0	January 21, 2025	Initial release
1.1	January 24, 2025	Updated Affected Software Versions list

The CVE-ID tracking this issue: CVE-2024-9135
CVSSv3.1 Base Score: 5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)
Common Weakness Enumeration: CWE-401: Missing Release of Memory after Effective Lifetime
This vulnerability is being tracked by BUG 1006114

Description

On affected platforms running Arista EOS with BGP Link State configured, BGP peer flap can cause the BGP agent to leak memory. This may result in BGP routing processing being terminated and route flapping.

This vulnerability was discovered externally and responsibly reported by Craig Dods from Meta's Infrastructure Security team.

Vulnerability Assessment

Affected Software

EOS Versions:

- 4.33.0
- 4.32.3 and below releases in the 4.32.x train
- 4.31.5 and below releases in the 4.31.x train
- 4.30.8.1 and below releases in the 4.30.x train
- 4.29.9.1 and below releases in the 4.29.x train
- All the releases in the 4.28.x train
- 4.27.1 and above releases in the 4.27.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
- 7010 Series
- 7010X Series
- 7020R Series
- 7130 Series running EOS
- 7170 Series
- 7060X/X2/X4/X5/X6 Series
- 7250X Series
- 7260X/X3 Series
- 7280R/R2/R3 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

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 eXchange, virtual or physical appliance
- CloudVision Portal, virtual appliance or physical appliance
- CloudVision as-a-Service
- CloudVision AGNI
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric and DANZ Monitoring Fabric (Formerly Big Switch Nodes for BCF and BMF)
- 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)
- Arista EOS-based End of Life platforms not supported on version 4.29 or later:
  - 7010T
  - 7300X
  - 7050X/X2

- 7160
- 7150
- 7280E/7500E

Required Configuration for Exploitation

In order to be vulnerable to CVE-2024-9135, the following condition must be met:

BGP Link State must be configured:

```
switch# router bgp 65544
switch#    address-family link-state
switch#       neighbor 192.0.2.9 activate
switch#
switch#sh bgp link-state summary
BGP summary information for VRF default
Router identifier 192.0.2.2, local AS number 65540
Neighbor Status Codes: m - Under maintenance
  Description              Neighbor V AS           MsgRcvd   MsgSent  InQ OutQ  Up/Do
wn State   NlriRcd NlriAcc

  brw363                   192.0.2.9 4 65550       194222    125149    0    0 01:08:4
1 Estab   211948 211948
```

If BGP Link State is not configured there is no exposure to this issue. No BGP link-state peering is shown under show bgp link-state summary as below:

```
switch>sh bgp link-state summary
BGP summary information for VRF default
Router identifier 192.0.2.2, local AS number 65540
Neighbor Status Codes: m - Under maintenance
  Description              Neighbor V AS           MsgRcvd   MsgSent  InQ OutQ  Up/Do
wn State   NlriRcd NlriAcc
```

Indicators of Compromise

This vulnerability may lead to low memory on the switch.

Mitigation

The workaround is to disable the Dynamic Path Selection (DPS) service inside BGP LinkState

by disabling the feature toggle. Note this should be done on affected non AWE platforms only.

```
1. Enter "bash" shell under EOS prompt
2. sudo sh -c 'echo "BgpLsConsumerDps=0" > /mnt/flash/toggle_override; echo "BgpLsPro
ducerDps=0" >> /mnt/flash/toggle_override'
3. Reload the switch or router
```

Hotfix

No hotfix exists 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-2024-9135 has been fixed in the following releases:

- 4.33.1 and later releases in the 4.33.x train
- 4.32.4 and later releases in the 4.32.x train
- 4.31.6 and later releases in the 4.31.x train
- 4.30.9 and later releases in the 4.30.x train
- 4.29.10 and later releases in the 4.29.x train

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).

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