**Date: July 22, 2025**

| Revision | Date | Changes |
|---|---|---|
| 1.0 | July 22, 2025 | Initial release |
| 1.1 | August 8, 2025 | Updated Mitigation section<br>Updated EOS versions which CVE-2025-6188 has been fixed |
| 1.2 | September 30, 2025 | Added CSAF file |

The CVE-ID tracking this issue: CVE-2025-6188
CVSSv3.1 Base Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)
Common Weakness Enumeration: CWE-288 Authentication Bypass Using an Alternate Path or Channel
This vulnerability is being tracked by BUG 1008073

# Description

On affected platforms running Arista EOS, maliciously formed UDP packets with source port 3503 may be accepted by EOS. UDP Port 3503 is associated with LspPing Echo Reply. This can result in unexpected behaviors, especially for UDP based services that do not perform some form of authentication.

This issue was discovered externally and responsibly reported to Arista by Chris Laffin of automattic.com. Arista is not aware of any malicious uses of this issue in customer networks.

# Vulnerability Assessment

## Affected Software

### EOS Versions

- 4.33.1F and below in the 4.33.X train
- 4.33.1.2F and below in the 4.33.1.X train
- 4.32.4.1M and below in the 4.32.X train
- 4.31.6M and below in the 4.31.X train
- 4.30.9.1M and below in the 4.30.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
    - 7150 Series
    - 7160 Series
    - 7170 Series
    - 7050X/X2/X3/X4 Series
    - 7060X/X2/X4/X5/X6 Series
    - 7250X Series
    - 7260X/X3 Series
    - 7280E/R/R2/R3 Series
    - 7300X/X3 Series
    - 7320X Series
    - 7358X4 Series
    - 7368X4 Series
    - 7388X5 Series
    - 7500E/R/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)

### Required Configuration for Exploitation

EOS devices are vulnerable to CVE-2025-6188 by default, and no specific configuration is necessary.

## Indicators of Compromise

No reliable ways exist to reliably identify if compromise has occurred.

## Mitigation

For EOS versions more recent than 4.28.1, if MPLS is not being used on the EOS device, a custom control plane ACL can be applied to remove the rules that allow traffic with source port 3503.

```
Switch(config)#system control-plane
Switch(config-cp)#ip access-group my-custom-acl
```

For EOS versions more recent than 4.22.0, an ‘mpls ping’ service ACL can be applied to restrict traffic coming with source/destination port 3503. This service ACL is applicable on the traffic coming in with source/destination port 3503. MPLS configuration is not required to apply the ACL.

Take the following example, where the user applies service ACL ‘Foo’ that allows traffic from 10.0.0.0/8 with source port 3503 and denies everything else.

```
Switch(config)#ip access-list Foo
Switch(config-acl-foo)#permit udp 10.0.0.0/8 eq lsp-ping any
Switch(config-acl-foo)#deny udp any eq lsp-ping any

Switch(config)#mpls ping
Switch(config-mpls-ping)#ip access-group foo in
```

If MPLS is not being used, it is fine to only have the deny rule in the ACL. For EOS versions older than 4.22.0 no mitigation exists.

## 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-2025-6188 has been fixed in the following releases:

- 4.34.0 and later releases in the 4.34.x train
- 4.33.2 and later releases in the 4.33.x train
- 4.32.5 and later releases in the 4.32.x train
- 4.31.7 and later releases in the 4.31.x train
- 4.30.10 and later releases in the 4.30.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