**Date: May 27, 2025**

| Revision | Date | Changes |
|---|---|---|
| 1.0 | May 27, 2025 | Initial release |
| 1.1 | June 4, 2025 | Updated Resolutions Section and Affected EOS Version |

The CVE-ID tracking this issue: CVE-2025-2796
CVSSv3.1 Base Score: 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)
Common Weakness Enumeration: CWE-284: Improper Access Control
This vulnerability is being tracked by BUG1073719

# Description

On affected platforms with hardware IPSec support running Arista EOS with IPsec enabled and anti-replay protection configured, EOS may exhibit unexpected behavior in specific cases. Received duplicate encrypted packets, which should be dropped under normal anti-replay protection, will instead be forwarded due to this vulnerability.

Note: this issue does not affect VXLANSec or MACSec encryption functionality.

This issue was discovered internally and Arista is not aware of any malicious uses of this issue in customer networks.

# Vulnerability Assessment

## Affected Software

### EOS Versions

- 4.34.0F
- 4.33.2F and below releases in the 4.33.x train

## Affected Platforms

The following products **are** affected by this vulnerability:

- Arista EOS-based products:
  - 7280R3 Series:
    - DCS-7280SR3AK, DCS-7280SR3AM

        - DCS-7280CR3AK, DCS-7280CR3AM
        - DCS-7280DR3AK, DCS-7280DR3AM
        - DCS-7289R3AK-BND, DCS-72789R3AM-BND and DCS-7289R3AK-SC, DCS-7289R3AM-SC
    - 7800R3 Series:

        - 7800R3A-36DM-LC, 7800R3AK-36DM-LC, 7800R3A-36PM-LC, 7800R3AK-36PM-LC

The following product versions and platforms **are not** 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 Series
    - 7280R3 and 7280R3A series not listed above, that do not support IPSec
    - 7300X/X3 Series
    - 7320X Series
    - 7358X4 Series
    - 7368X4 Series
    - 7388X5 Series
    - 7500E/R/R2/R3 Series
    - 7800R3 and 7800R3A series not listed above, that do not support IPSec
    - 7800R4 Series
    - 7700R4 Series
    - AWE 5000 Series
    - AWE 7200R Series
    - CloudEOS
    - cEOS-lab
    - vEOS-lab
    - CloudVision eXchange, virtual or physical appliance
- Arista Wireless Access Points
- CloudVision CUE, virtual appliance or physical appliance
- CloudVision CUE cloud service delivery

- CloudVision Portal, virtual appliance or physical appliance
- CloudVision as-a-Service
- CloudVision AGNI
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric (formerly Big Switch BCF)
- Arista DANZ Monitoring Fabric (formerly Big Switch 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

In order to be vulnerable to CVE-2025-2796, the following condition must be met:

**anti-replay detection** must be configured in IPSec SA Policy:

```
switch(config)# ip security
switch(config-ipsec)# sa policy sa1
switch(config-ipsec-sa1)# anti-replay detection
```

## Indicators of Compromise

No practical ways exist to determine if the system has been compromised.

## Mitigation

There is no known mitigation for CVE-2025-2796. The recommended resolution is to upgrade to a remediated software version at your earliest convenience.

## 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-2025-2796 has been fixed in the following releases:

- 4.33.3F 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

Contact information needed to open a new service request may be found at:

https://www.arista.com/en/support/customer-support