Date: December 30, 2025

Revision	Date	Changes
1.0	December 30, 2025	Initial release
1.1	February 3, 2026	Updated Required Configuration for Exploitation

The CVE-ID tracking this issue: CVE-2025-7048
CVSS:3.1 Base Score 4.3 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)
CVSS:4.0 Base Score 5.3
(CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-805 Buffer Access with Incorrect Length Value
This vulnerability is being tracked by BUG1153233, BUG1203696

Description

On affected platforms running Arista EOS with MACsec configuration, a specially crafted packet can cause the MACsec process to terminate unexpectedly. Continuous receipt of these packets with certain MACsec configurations can cause longer term disruption of dataplane traffic.

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

Vulnerability Assessment

Affected Software

EOS Versions

- 4.34.3.1M and earlier releases in the 4.34.x train
- 4.33.5M and earlier releases in the 4.33.x train
- 4.32.7M and earlier releases in the 4.32.x train
- 4.31.9M and earlier releases in the 4.31.x train
- 4.30.x and all earlier releases with MACsec support

Affected Platforms

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

- Arista EOS-based products that support MACsec:
  - 7388-8D Series
  - 7500R/R2 Series
  - 7800/R3/R3A Series

    - 722XPM and 720XPM Series
    - 750X Series
    - 7050X3/X4 Series
    - 7170 Series
    - 7280R/R2/R3/R3A/R4 Series
    - 7289R3 Series
    - cEOS-lab
    - vEOS-lab

The following product versions and platforms **are not** affected by this vulnerability:

- Arista EOS-based products
    - 710 Series
    - 720D Series
    - 720XP Series
    - 750X Series
    - 7010 Series
    - 7010X Series
    - 7020R Series
    - 7130 Series running EOS
    - 7150 Series
    - 7160 Series
    - 7050X/X2 Series
    - 7060X/X2/X4/X5/X6 Series
    - 7250X Series
    - 7260X/X3 Series
    - 7280E Series
    - 7280R4 Series
    - 7300X/X3 Series
    - 7320X Series
    - 7358X4 Series
    - 7368X4 Series
    - 7388/16CD/16CD2/8DR/SUP/SUP-D-X5-SC/X5 Series
    - 7500R3 Series
    - 7800R4 Series
    - 7700R4 Series
    - AWE 5000 Series
    - AWE 7200R Series
    - CloudEOS
    - 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)
- 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-2025-7048, the following condition must be met:

MACsec must be configured on one or more interfaces:

Below show command output having a non-zero ‘Active Profiles:’ represents some of the interfaces are configured with MACsec

```
switch#show mac security participants
Administrative State:     enabled
Active Profiles:          2
Data Delay Protection:    no
EAPoL Destination MAC:    0180.c200.0003
FIPS Mode:                no
Secured Interfaces:       2
License:                  enabled
```

If MACsec is not configured on any of the interfaces (ie, Active Profiles are zero), there is no exposure to the issue mentioned in this advisory.

Indicators of Compromise

This vulnerability may lead to unexpected MACsec agent restart on the switch.

The following message may appear in “**show logging**”:

```
Jul 15 01:56:55 switch ProcMgr: %PROCMGR-6-PROCESS_TERMINATED: 'Macsec' (PID=13153, s
tatus=-6) has terminated.
Jul 15 01:56:55 switch ProcMgr: %PROCMGR-6-PROCESS_RESTART: Restarting 'Macsec' immed
iately (it had PID=13153)
```

Backtrace with following signature may appear in /var/log/agents/Macsec-<PID> (This requires bash access):

The following log indicates that the MACsec agent received a malformed packet on a MACsec-enabled interface and crashed while attempting to interpret the packet.

```
BUG1153233:
-----------
Macsec: /src/tacc/Fwk/Cpp/Tac/AllocTrackImpl.h:276: : Assertion `!overflow && "AllocT
rackOverflow"' failed.

---------- BEGIN MANTLE DUMP ----------
Generated at Tue Jul 15 01:56:43 2025, -0700 (PDT). NOTE: Use 'log2core' to convert t
his log file to a debuggable core.
Command: Macsec
Arguments: Macsec
Assertion Failure: /src/tacc/Fwk/Cpp/Tac/AllocTrackImpl.h:276: !overflow && "AllocTra
ckOverflow"
Unix Time: 1752569803: Process 13153 lwp 13153 died with signal 6 (SIGABRT) code -6 (
Sent by process 13153 running with user id 0)
```

The following log indicates that an encrypted parameter in the received packet was malformed which results in the termination of the MACsec agent.

```
BUG1203696:
-----------
2025-07-15 03:58:45.267972  8418 Macsec               1 Fn: 'keyUnwrap', error: 'AES_
unwrap_key failed'
2025-07-15 03:58:45.268109  8418 Macsec               1 CRYPTOLIB_ERROR: Exception ra
ised inside keyUnwrap
Macsec: /src/MacsecCommon/crypto.cpp:33: void Macsec::handleErrors(const char*): Asse
rtion `false' failed.

---------- BEGIN MANTLE DUMP ----------
Generated at Tue Jul 15 03:58:45 2025, -0700 (PDT). NOTE: Use 'log2core' to convert t
his log file to a debuggable core.
Command: Macsec
Arguments: Macsec
Assertion Failure: /src/MacsecCommon/crypto.cpp:33 in void Macsec::handleErrors(const
 char*): false
Unix Time: 1752577125: Process 8418 lwp 8418 died with signal 6 (SIGABRT) code -6 (Se
```

```
nt by process 8418 running with user id 0)
```

When the agent restarts MACsec core files will be generated in /var/core. Existence of this file indicates that the agent restarted.

```
core.<PID>.<time-stamp>.Macsec.gz
```

Mitigation

There is no known work around to keep MACsec running and make it not susceptible to the security issue. MACsec would need to be disabled to eliminate the 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-2025-7048 has been fixed in the following releases:

- 4.35.0F and later releases
- 4.34.4M and later releases in the 4.34.x train
- 4.33.6M and later releases in the 4.33.x train
- 4.32.8M and later releases in the 4.32.x train
- 4.31.10M and later releases in the 4.31.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) 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