Date: April 8, 2025

Revision	Date	Changes
1.0	April 8, 2025	Initial release

The CVE-ID tracking this issue: CVE-2024-12378
CVSSv3.1 Base Score: 9.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N)
Common Weakness Enumeration: CWE-319: Cleartext Transmission of Sensitive Information
This vulnerability is being tracked by BUG 997526

Description

On affected platforms running Arista EOS with secure Vxlan configured, restarting the Tunnelsec agent will result in packets being sent over the secure Vxlan tunnels in the clear.

Arista is not aware of any malicious uses of this issue in customer networks.

Vulnerability Assessment

Affected Software

EOS Versions

- 4.32.2F and below releases in the 4.32.x train
- 4.31.6M and below releases in the 4.31.x train
- 4.30.8M and below releases in the 4.30.x train
- 4.29.9M and below releases in the 4.29.x train
- 4.28.12M and below releases in the 4.28.x train
- 4.27.12M and below releases in the 4.27.x train

Affected Platforms

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

- Arista EOS-based products:
  - 7280CR3MK Series as below:
    - 7280CR3MK-32P4
    - 7280CR3MK-32P4S
    - 7280CR3MK-32D4S
    - 7280CR3MK-32D4A

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 Series
    - 7250X Series
    - 7260X/X3 Series
    - 7280E/R/R2 Series
    - 7280R3 Series not explicitly listed above
    - 7300X/X3 Series
    - 7320X Series
    - 7358X4 Series
    - 7368X4 Series
    - 7388X5 Series
    - 7500E/R/R2/R3 Series
    - 7800R3 Series
    - CloudEOS
    - cEOS-lab
    - vEOS-lab
    - AWE 5000 Series
- 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

In order to be vulnerable to CVE-2024-12378, the following condition must be met:

Secure Vxlan must be configured.

The output of “show ip security connection” is empty if Secure Vxlan isn’t configured.

```
switch> show ip security connection
Legend: (P) policy based VPN tunnel
Tunnel                    Source      Dest        Status        Uptime      Input
Output     Rekey       Time
vxlansec-
default-1.0.2.1 1.0.1.1     1.0.2.1     Established
     19 minutes  0 bytes   152 bytes              24 minutes
                                                                          0 pkts
2 pkts
```

A normal encrypted connection will show the status as “established”.

Indicators of Compromise

The secure Vxlan tunnel will go from Established to Connected state, but packets will be sent and received successfully over the tunnel.

```
switch> show ip security connection
Legend: (P) policy based VPN tunnel
Tunnel                    Source      Dest         Status       Uptime     Input
Output     Rekey       Time
vxlansec-
default-1.0.2.1 1.0.1.1     1.0.2.1      Connected
    N/A        0 bytes    0 bytes                N/A
                                                                        0 pkts
0 pkts
```

Mitigation

The workaround is to remove and re-apply security profiles for each secure VTEP.

```
switch> show vxlan security profile
VTEP          Security Profile
```

```
------------ ----------------
1.0.2.1                    p1
switch> en
switch# config
switch(config)# interface vxlan 1
switch(config-if-Vx1)# no vxlan vtep 1.0.2.1 ip security profile p1
switch(config-if-Vx1)# vxlan vtep 1.0.2.1 ip security profile p1
```

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-2024-12378 has been fixed in the following releases:

- 4.33.0F and later releases in the 4.33.x train
- 4.32.3M and later releases in the 4.32.x train
- 4.31.7M and later releases in the 4.31.x train
- 4.30.9M and later releases in the 4.30.x train
- 4.29.10M and later releases in the 4.29.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