Date: November 19, 2024

Revision	Date	Changes
1.0	November 19, 2024	Initial release

The CVE-ID tracking this issue: CVE-2024-7095
CVSSv3.1 Base Score: 4.3 (CVSS:3.1/AV:N/AC:L/PR:L/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 BUG974415

Description

On affected platforms running Arista EOS with SNMP configured, if "**snmp-server transmit max-size**" is configured, under some circumstances a specially crafted packet can cause the snmpd process to leak memory. This may result in the snmpd process being terminated (causing SNMP requests to time out until snmpd is restarted) and memory pressure for other processes on the switch. Increased memory pressure can cause processes other than snmpd to be at risk for unexpected termination as well.

This was discovered internally by Arista and we are 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
- 4.31.4M and below releases in the 4.31.x train
- 4.30.7M and below releases in the 4.30.x train
- 4.29 train (all releases)
- 4.28 train (all releases)
- 4.27 train (all releases)
- 4.26 train (all releases)
- 4.25 train (all releases)
- 4.24 train (all releases)
- 4.23 train (all releases)
- 4.22 train (all releases)

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 Series
    - AWE 5000 Series
    - AWE 7200R Series
    - CloudEOS
    - cEOS-lab
    - vEOS-lab
    - CloudVision eXchange, virtual or physical appliance

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

In order to be vulnerable to CVE-2024-7095, the following conditions must be met:

1. SNMP must be configured, and
2. "**snmp-server transmit max-size**" must be configured

If the necessary configurations are present, **show snmp** output will look something like below, where **Transmit message maximum size** will contain a number smaller than the default of 65536:

```
switch>show snmp
Chassis: None
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
0 SNMP packets output
    0 Too big errors
    0 No such name errors
    0 Bad value errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
    0 Trap drops
Access Control
    0 Users
    0 Groups
    0 Views
SNMP logging: disabled
SNMP agent enabled in VRFs: default
Transmit message maximum size: 1500
```

If SNMP is not configured there is no exposure to this issue and the **show snmp** output will look something like:

```
switch>show snmp
Chassis: XXXXXXXXXXX
SNMP agent enabled in VRFs: default
Transmit message maximum size: 65536
SNMP agent disabled:
 Either no communities and no users are configured, or no VRFs are configured.
```

If the **transmit max-size** is not configured there is no exposure to this issue and even if SNMP is configured, the **show snmp** output will look something like:

```
switch>show snmp
Chassis: None
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
0 SNMP packets output
    0 Too big errors
    0 No such name errors
    0 Bad value errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
    0 Trap drops
Access Control
    0 Users
    0 Groups
    0 Views
SNMP logging: disabled
SNMP agent enabled in VRFs: default
Transmit message maximum size: 65536
```

Indicators of Compromise

This vulnerability may lead to low memory on the switch.

The snmpd process may show ever-increasing memory consumption; subsequent runs of the following command will show ever-increasing values:

```
switch#show processes top once | grep snmpd | awk ''
7476
switch#show processes top once | grep snmpd | awk ''
7596
switch#show processes top once | grep snmpd | awk ''
7604
```

The snmpd process being terminated due to out of memory may be an indication of the issue. The following message may appear in **show logging**:

```
Jan 1 00:00:41 switch SuperServer: %SYS-4-RESTART_SERVICE: Service snmpd is not runni
ng. Attempting to restart it.
```

The following kernel message may also appear under “/var/log/eos” (this requires bash access) which indicates the issue:

```
Jan 1 00:00:14 switch kernel: [12034.891
991] Out of memory: Killed process 5374 (snmpd) total-vm:1711408kB, anon-rss:1698956k
B, file-rss:4084kB, shmem-rss:0kB, UID:0 pgtables:3376kB oom_score_adj: -300  memory-
usage:42.4% oom_score:124
```

These messages can be found with the following grep commands, when run from the bash shell:

```
grep "Out of memory: Killed process [0-9]* (snmpd)" /var/log/eos
grep "Service snmpd is not running. Attempting to restart it." /var/log/eos
```

Mitigation

The workaround is to disable **snmp-server transmit max-size** configuration:

```
no snmp-server transmit max-size
```

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-2024-7095 has been fixed in the following releases:

- 4.32.3M and later releases in the 4.32.x train
- 4.31.5M and later releases in the 4.31.x train
- 4.30.8M 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