Date: April 11, 2023

Revision	Date	Changes
1.0	April 11, 2023	Initial release

The CVE-ID tracking this issue: CVE-2023-24511
CVSSv3.1 Base Score: 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/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 BUG 751040

Description

On affected platforms running Arista EOS with SNMP configured and the snmpd process is running, a specially crafted SNMP packet can cause a memory leak in the snmpd process. This may result in the snmpd processing being terminated (causing SNMP requests to time out until snmpd is automatically restarted) and potential memory resource exhaustion for other processes on the switch. The vulnerability does not have any confidentiality or integrity impacts to the system.

The vulnerability was reported externally by an Arista customer. Arista is not aware of any malicious uses of this issue in customer networks.

Vulnerability Assessment

Affected Software

EOS Versions

- 4.29.1F and below releases in the 4.29.x train
- 4.28.5.1M and below releases in the 4.28.x train
- 4.27.8.1M and below releases in the 4.27.x train
- 4.26.9M and below releases in the 4.26.x train
- 4.25.10M and below releases in the 4.25.x train
- 4.24.11M and below releases in the 4.24.x train

Affected Platforms

This is a platform-independent vulnerability and affects all systems running EOS with the versions identified above. The following products **are** affected by this vulnerability:

- Arista EOS-based products:
    - 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/R3 Series
- 7300X/X3 Series
- 7320X Series
- 7358X4 Series
- 7368X4 Series
- 7388X5 Series
- 7500E/R/R2/R3 Series
- 7800R3 Series
- CloudEOS
- cEOS-lab
- vEOS-lab

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

- Arista Wireless Access Points
- CloudVision WiFi, virtual appliance or physical appliance
- CloudVision WiFi cloud service delivery
- CloudVision Portal, virtual appliance or physical appliance
- CloudVision as-a-Service
- 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 Unified Cloud Fabrics - (Formerly Pluribus Netvisor One)

Required Configuration for Exploitation

In order to be vulnerable to CVE-2023-24511, the following condition must be met:

SNMP must be configured:

```
switch>show snmp
Chassis: XXXXXXXXXXX
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
Access Control
    0 Users
    0 Groups
    0 Views
SNMP logging: disabled
SNMP agent enabled in VRFs: default
Transmit message maximum size: 65536
```

If SNMP is not configured there is no exposure to this issue and the message 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 ar
e configured.
```

Indicators of Compromise

This vulnerability may lead to low memory on the switch.

The snmpd process being terminated 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.
```

If the first message is seen, the following confirms this was the result of running out of memory. The following kernel message may also appear under “/var/log/eos” (this requires bash access) which indicates acts as the second indicator:

```
Jan 1 00:00:14 switch kernel: [12034.891991] Out of memory: Killed process 5374 (snmp
d) total-vm:1711408kB, anon-rss:1698956kB, 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

If you suspect you are encountering this issue due to malicious activity, the workaround is to enable SNMP service ACLs to only allow specific IP addresses to query SNMP (combined with anti-spoofing ACLs in the rest of the network).

```
snmp-server ipv4 access-list allowHosts4
snmp-server ipv6 access-list allowHosts6
!
ipv6 access-list allowHosts6
   10 permit ipv6 host <ipv6 address> any
!
ip access-list allowHosts4
   10 permit ip host <ipv4 address> any
```

For more information about SNMP service ACLs see EOS User Manual: SNMP IP Address ACL Support.

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-2023-24511 has been fixed in the following releases:

- 4.29.2F and later releases in the 4.29.x train
- 4.28.6M and later releases in the 4.28.x train
- 4.27.9M and later releases in the 4.27.x train
- 4.26.10M and later releases in the 4.26.x train

Hotfix

The following hotfix can be applied to remediate CVE-2023-24511. The hotfix only applies to the releases listed below and no other releases. All other versions require upgrading to a release containing the fix (as listed above).:

- 4.29.1F and below releases in the 4.29.x train
- 4.28.5.1M and below releases in the 4.28.x train
- 4.27.8.1M and below releases in the 4.27.x train
- 4.26.9M and below releases in the 4.26.x train

Note: Installing/uninstalling the SWIX will cause the snmpd process to restart

Version: 1.0

URL: SecurityAdvisory84_CVE-2023-24511_Hotfix.swix

SWIX hash: SecurityAdvisory84_CVE-2023-24511_Hotfix.swix

```
(SHA-512)da2bc1fd2c7fc718e3c72c7ce83dc1caa05150cbe2f081c8cc3ed40ce787f7e24dff5202e621
ef5f2af89f72afd25f7476d02f722ffe8e8c7d24c101cbbfe0e5
```

For instructions on installation and verification of the hotfix patch, refer to the “managing eos extensions” section in the EOS User Manual. Ensure that the patch is made persistent across reboots by running the command ‘copy installed-extensions boot-extensions’.

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

By email: support@arista.com
By telephone: 408-547-5502 ; 866-476-0000
Contact information needed to open a new service request may be found at:
https://www.arista.com/en/support/customer-support