Date: May 31, 2023

Revision	Date	Changes
1.0	May 31, 2023	Initial release

The CVE-ID tracking this issue: CVE-2023-24510
CVSSv3.1 Base Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
Common Weakness Enumeration: CWE-755 Improper Handling of Exceptional Conditions
This vulnerability is being tracked by BUG753188

Description

On the affected platforms running EOS, a malformed DHCP packet might cause the DHCP relay agent to restart.

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

Vulnerability Assessment

Affected Software

EOS Versions

This issue was introduced in EOS version 4.20.5.

- 4.29.1F and below releases in the 4.29.x train
- 4.28.6.1M and below releases in the 4.28.x train
- 4.27.9M 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
- Note: While earlier EOS software versions may be affected, EOS software trains 4.24 and earlier have reached end of support and are no longer maintained.

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 eXchange, virtual or physical appliance
- 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)

Required Configuration for Exploitation

In order to be vulnerable to CVE-2023-24510, the following condition must be met:

- – At least two “ip helper-address” commands for the DHCP server are configured on the

same interface.
- – Scenario One:
  - – One command uses “source-interface”, with or without being in a VRF.
  - – The second command does not use a source-interface and does not use a VRF.
- – Scenario Two:
  - – One command is run inside of a VRF.
  - – The second command does not use a source-interface and does not use a VRF.

The below configuration sample shows two VLAN interfaces which will be exposed to the issue:

```
interface Vlan11
   ip helper-address 100.1.1.2 [vrf blue] source-interface Loopback1
   ip helper-address 50.1.1.2

 interface Vlan12
   ip helper-address 100.1.1.2 vrf blue
   ip helper-address 50.1.1.2
```

Indicators of Compromise

The impact of this vulnerability is that the DHCP relay agent would restart.

The following message will appear in “show logging” to indicate the restart:

```
Apr 27 03:30:59 switch ProcMgr-worker: %PROCMGR-6-PROCESS_RESTART: Res
tarting 'DhcpRelay' immediately (it had PID=4107)
Apr 27 03:30:59 switch ProcMgr-worker: %PROCMGR-7-PREDECESSOR_WAITING:
 New instance of DhcpRelay (PID=5103): waiting for reaping of predeces
sor (PID=4107)
Apr 27 03:30:59 switch ProcMgr-worker: %PROCMGR-7-PREDECESSOR_GONE: Ne
w instance of DhcpRelay (PID=5103): predecessor (PID=4107) has been re
aped.
Apr 27 03:30:59 switch ProcMgr-worker: %PROCMGR-6-PROCESS_STARTED: 'Dh
cpRelay' starting with PID=5103 (PPID=1949) -- execing '/usr/bin/DhcpR
elay'
Apr 27 03:30:59 switch DhcpRelay: %AGENT-6-INITIALIZED: Agent 'DhcpRel
ay' initialized; pid=5103
```

Mitigation

There is no known mitigation for this issue.

Resolution

The recommended resolution is to upgrade to a remediated software version at your earliest convenience. Artista 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-2023-24510 has been fixed in the following releases:

- 4.29.2F and later releases in the 4.29.x train
- 4.28.7M and later releases in the 4.28.x train
- 4.27.10M 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-2023-24510. 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
- 4.28.6.1M and below releases in the 4.28.x train
- 4.27.9M 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

Note: Installing/uninstalling the SWIX will cause the DHCP relay agent to restart

Verizon: 1.0

URL: SecurityAdvisory87_Hotfix.swix

SWIX hash:

```
(SHA-512)fc9051ad9a83c7b507d843bebc4964259f68ae0a7dfb4783680d44b8eda07
```

```
8a5f3a7041e584bc4508480197fb4f8d27da39f87c45e6f98f0d839a5240a48f71f
```

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