Date: October 7th, 2020

Version: 1.0

Revision	Date	Changes
1.0	October 7th, 2020	Initial Release

The CVE-ID tracking this issue is: CVE-2020-17355
CVSSv3 Base Score: 7.5/10 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Description

This advisory documents a security vulnerability in Arista EOS, for customers who leverage DHCPv6 with a specific relay option configured. The vulnerability is found in EOS where a malformed DHCP packet can lead to an incorrect route being installed. This incorrect route in turn may result in a restart of agents attempting to process the route.

The impact, in the form of agent restarts or feature usability, would be specific to the SandL3Unicast, Ira, Arp, or Snmp agents. The exposure is limited to devices with the option for “ipv6 dhcp relay install routes” configured, with the malformed packet directed on a routed port that DHCP Relay is listening on.

Arista has not received any report of this issue being exploited in any malicious manner.

Symptoms

It is required for the “ipv6 dhcp relay install routes” configuration line to be applied for this vulnerability to be exploited. If the vulnerability has been exploited, the symptoms of this attack would be an agent restart of SandL3Unicast, Ira, Arp, or Snmp. Agent restarts are logged under **show logging all**.

Example 1:

```
ProcMgr-worker: %
PROCMGR-6-PROCESS_TERMINATED
: ‘'SandL3Unicast' (PID=4609) has terminated.
ProcMgr-worker:  %PROCMGR-6-PROCESS_RESTART: Restarting 'SandL3Unicast
' immediately (it had PID=4609) 2020 Sep 21 04:23:22
ProcMgr-worker: %PROCMGR-6-PROCESS_STARTED: 'SandL3Unicast' starting w
ith PID=28332 (PPID=2419) -- execing '/usr/bin/SandL3Unicast'``
```

Copyright 2025 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

Example 2:

```
ProcMgr-worker: %PROCMGR-4-TERMINATE_PROCESS_SIGQUIT: Heartbeats from
'Snmp' (PID=18833) missing for 61.0 secs -- terminating it with SIGQUI
T
ProcMgr-worker:    %
PROCMGR-6-PROCESS_TERMINATED: 'Snmp' (PID=18833) has terminated.
ProcMgr-worker: %PROCMGR-6-PROCESS_RESTART: Restarting 'Snmp' immediat
ely (it had PID=18833)
ProcMgr-worker:  %PROCMGR-6-PROCESS_STARTED: 'Snmp' starting with PID=
24521 (PPID=2257) -- execing '/usr/bin/Snmp'
```

The “%PROCMGR-6-PROCESS_TERMINATED” log highlighted above indicates that the agent has crashed.

Vulnerability Assessment

Affected Software

- EOS:
  - 4.24.1F and below release in the 4.24.x train
  - 4.23.4M and below releases in the 4.23.x train
  - 4.22.6M and below releases in the 4.22.x train
  - 4.21.11M and below releases in the 4.21.x train
  - 4.20.1F and above releases in the 4.20.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 **not affected:**
  - Arista Wireless Access Points
  - CloudVision Wi-Fi, virtual appliance or physical appliance
  - CloudVision Wi-Fi cloud service delivery
  - CloudVision Portal, virtual appliance or physical appliance
  - CloudVision as-a-Service
  - CloudEOS Virtual Router, as a VM on-premises or in the public cloud marketplaces
  - CloudEOS Container, that runs in Kubernetes on-premises clusters
  - Arista 7130 Systems running MOS
  - Arista CCF (Converged Cloud Fabric) and DMF (DANZ Monitoring Fabric)

Copyright 2025 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

(formerly Big Switch Nodes for BCF and BMF)

Mitigation

As a security best practice, it is recommended to restrict public access to DHCP servers or any other internal devices sending DHCPv6 packets. Additionally, an Access-Control list (ACL) can be configured on the port that DHCP is listening on, on the EOS switch, allowing access to and from trusted DHCP servers only. For the final resolution, refer to the next section for remediated software versions.

As a workaround, “ipv6 dhcp relay install routes” can be removed from the configuration to safeguard against this vulnerability until a fix is installed.

Resolution

This vulnerability is being tracked by Bug 498246. To safeguard against this vulnerability, the recommended course of action is to perform an upgrade to a remediated EOS version.

The vulnerability has been fixed in the following EOS versions:

- 4.24.2F
- 4.23.5M
- 4.22.7M
- 4.21.12M

For users exposed to this vulnerability who are unable to upgrade EOS to leverage the resolution and need a temporary fix, contact your Arista Account team or Arista TAC for assistance.

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

Copyright 2025 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.