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-2020-15897
CVSSv3.1 Base Score: 6.5 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Description

This advisory documents the impact of a vulnerability in Arista's EOS, specifically the routing process when malformed packets are received by IS-IS. Systems that do not have IS-IS configured are not impacted by this vulnerability.

The effect of the vulnerability is dependent on the routing protocol mode configuration. The IS-IS protocol (in Multi-Agent mode) or all layer 3 protocols (in Ribd, single routing agent mode) can be affected if the IS-IS Router receives a malformed link-state PDU. The effect will be agent restarts (Rib process or IS-IS process, depending on the routing protocol mode) that could trigger route churn, which may subsequently result in traffic loss or incorrect forwarding of traffic.

This is an internally found vulnerability and Arista has not received any report of this issue being used in any malicious manner.

Symptoms

Arista EOS can use single routing agent mode (Ribd) or multi-agent mode. Both modes are vulnerable, with the impact depending on the mode in use. The routing agent mode relates to which agent could restart when the malformed PDU is received. The following checks can be performed to confirm if this vulnerability has been hit:

1) Confirm the routing mode configured on the Router in question via the command **show running all | grep "service routing protocols model"**:

Example(s) of vulnerable configuration:

Ribd mode

```
service routing protocols model ribd
```

Multi-agent mode

```
service routing protocols model multi-agent
```

The setting in use relates to the protocols impacted. If the model setting is "ribd", all layer-3 protocols can be affected. If the mode setting is "multi-agent", only the IS-IS protocol will be affected when the vulnerability is exploited.

2) Observe the following logs after running **show logging all** on the device in question.

Example(s):

Ribd mode

```
ProcMgr-worker: %PROCMGR-6-PROCESS_TERMINATED: 'Rib' (PID=2245) has terminated.
ProcMgr-
worker: %PROCMGR-6-PROCESS_RESTART: Restarting 'Rib' immediately (it had PID=2245)
ProcMgr-worker: %PROCMGR-6-PROCESS_STARTED: 'Rib' starting with PID=691 (PPID=1699) -
- execing '/usr/bin/Rib'
```

Multi-agent mode

```
ProcMgr-
worker: %PROCMGR-6-PROCESS_TERMINATED: 'Isis' (PID=2666, status=139) has terminated.
ProcMgr-
worker: %PROCMGR-6-PROCESS_RESTART: Restarting 'Isis' immediately (it had PID=2666)
ProcMgr-worker: %PROCMGR-6-PROCESS_STARTED: 'Isis' starting with PID=4014 (PPID=1916)
 -- execing '/usr/bin/Isis'
```

If the above logs are continuously recorded, it indicates that the Rib/IS-IS agent may be experiencing ongoing crashes.

3) If Rib/IS-IS restarts have been observed in the previous step, the following backtrace should be observed after running show agent logs crash | grep "isis_pdu_parse_xngb_subtlvs" on the device in question:

Example:

```
/lib64/libgated_all.so(isis_pdu_parse_xngb_subtlvs+0x5dc)[0x7f27a1211a2c]
```

The highlighted segment of the crash log is relevant to this vulnerability. This check is applicable to both Ribd and Multi-agent routing modes.

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.
  - 4.21.10M and below releases in the 4.21.x train.
  - All 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
  - Arista 7130 Systems running MOS
  - Arista Converged Cloud Fabric and DANZ Monitoring Fabric (Formerly Big Switch Nodes for BCF and BMF)

Mitigation

IS-IS supports MD5 authentication, which can be leveraged as a mitigation step to limit the set of devices from which one will be able to accept IS-IS PDUs. For details on how to configure IS-IS MD5 authentication, please refer to the EOS manual:

https://www.arista.com/en/um-eos/eos-section-35-2-is-is#ww1232672

In addition, network designs should separate the IS-IS control plane from any untrusted data plane. For the final resolution, please refer to the next section which lists the details of the remediated software versions.

Resolution

This vulnerability is tracked by Bug 497449. The recommended resolution is to 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 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