Date: November 6th, 2019

Version: 1.0

Revision	Date	Changes
1.0	November 6th, 2019	Initial Release

The CVE-IDs tracking this issue: CVE-2019-9512, CVE-2019-9514, and CVE-2019-9515

CVSSv3 Base Score: 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Description

This advisory documents the exposure of Arista's products to the above-listed CVEs regarding an HTTP2 OOM security vulnerability in Go's gRPC library. The vulnerability is in an open-source software, Go's gRPC library, and Arista has not received evidence of this vulnerability being exploited, as of the date of initial release of this advisory.

- **EOS** - In EOS, the exposure is limited to the state streaming components - TerminAttr and OpenConfig. Arista's EOS eAPI software does not use HTTP2 and is not affected. TerminAttr and OpenConfig are shipped natively with EOS but are not enabled by default. If either service is enabled, the service will be affected by this security vulnerability.
- **MOS (7130 Series)** - MOS does not have HTTP2 enabled and is not affected
- **CloudVision Portal** - The ingest component in the CVP Backend is affected
- **Wi-Fi software** - Access Points with OpenConfig interface enabled are vulnerable. Openconfig is disabled by default on the Access Points and there is no impact unless it is explicitly enabled. The OpenConfig interface is authenticated and credentials are required to extend the exploit. None of the other Wi-Fi software components including the wireless manager and the cloud services are impacted by this vulnerability.

If TerminAttr or OpenConfig is enabled, an attacker could continually send data/flood that could cause the TerminAttr or OpenConfig agent to consume large amounts of memory, potentially leading to an OOM (Out of Memory) condition.

Symptoms

The exploitation of this vulnerability can lead to an Out-of-Memory condition on the impacted device. Repeated attempts could potentially lead to a Denial of Service attack as other agents can run out of memory due to large memory consumption by TerminAttr and/or Openconfig agents.

Vulnerability Assessment

Affected Software

- TerminAttr:
  - v1.6.0
  - v1.5.x: 1.5.9 and below
- OpenConfig (shipped natively in EOS):
  - 4.23 release train: 4.23.0F
  - 4.22 release train: 4.22.2F and earlier releases
  - 4.21 release train: 4.21.7.1M and earlier releases
  - 4.20 release train: 4.20.14M and earlier releases
  - 4.19 release train: 4.19.13M and earlier releases
  - End of support release trains (4.18 and 4.17)
- CloudVision Portal (CVP):
  - 2018.2.5 and earlier releases
- Wi-Fi:
  - 8.7.3-26 and earlier versions

Affected Platforms

- This is a platform-independent vulnerability

Mitigation

As a security best practice, it is recommended to not expose internal devices to public access to safeguard from potential attacks. As a resolution against this vulnerability, refer to the next section for a hitless hotfix for EOS and code upgrade path for all products.

Resolution

The vulnerability is tracked by:

- TerminAttr: BUG409659 and BUG416064
- OpenConfig: BUG409658 and BUG416066
- Wi-Fi Access Points: BUG414149

EOS with TerminAttr enabled - The recommended course of action is to upgrade TerminAttr to a fixed version. Upgrading TerminAttr to a remediated version is non-disruptive to the device operation or traffic forwarding, and addresses this vulnerability for EOS and CloudVision Portal. During the TerminAttr update, the connection of CVP to devices is reset and streaming telemetry is buffered until TerminAttr is running again and the connection is re-established. Arista suggests leveraging CVP to upgrade TerminAttr across all devices.

EOS with OpenConfig enabled - For OpenConfig, install the provided hotfix for immediate resolution. Hotfix install instructions for OpenConfig in EOS:

- The hotfix can be installed as an EOS extension on the specific versions listed below
- The hotfix restarts the OpenConfig agents which will reset/reestablish any open connections, but there is no impact on traffic or device operation.

(1) Patch file download URL: SecurityAdvisory0043Hotfix-1-v1.0.0.swix

sha512 checksum for verification: be17fce400045ee63c7d77cb756e47aebf460c878793b1984ed3c79f7c3be3ec189c986afdcbc3d1814170d2e1f5c594b3ac7d179ebe05eda05c4919d9789036

This patch is compatible with the following EOS versions:

- 4.20.11M
- 4.20.11.1M
- 4.20.12M
- 4.20.12.1M
- 4.20.13M
- 4.20.13.1M
- 4.20.14M
- 4.21.7M
- 4.21.7.1M
- 4.21.8M

(2) Patch file download URL: SecurityAdvisory0043Hotfix-2-v1.0.0.swix

sha512 checksum for verification: ef84fb5e4eb2ffe9f1cf2904cb1b496fb115c444de21f4cf38858daa4a0cba35a6cad9677d01b8f1885df42ff15368c864998eb4afcc7625e39195e08f65c669

This patch is compatible with the following EOS versions:

- 4.22.0F
- 4.22.0.1F
- 4.22.0.2F
- 4.22.1F
- 4.22.2F
- 4.23.0F
- 4.23.0.1F

For instructions on installation and verification of EOS extensions, refer to this section in the EOS User Manual: https://www.arista.com/en/um-eos/eos-section-6-7-managing-eos-extensions. Ensure that the extension is made persistent across reboots by copying the installed-extensions to boot-extensions.

After the patch is in place, a log message is recorded to highlight any attack if there might be an attempt to exploit this vulnerability

```
 kernel: [ 7458.218363] TCP: request_sock_TCP: Possible SYN flooding on port 6042. Sending cookies. Check SNMP counters.
```

CloudVision - The vulnerability is addressed in the 2019.1.0 and later versions of CloudVision Portal. Updating TerminAttr on managed devices protects against this vulnerability on affected CloudVision Portal releases.

Wi-Fi Access Points - If OpenConfig is explicitly enabled, the recommendation is to upgrade to a remediated code version, v8.8.1, to safeguard against this vulnerability.

The vulnerability is fixed in the following versions:

- TerminAttr:
  - v1.7.1 and above
  - v1.5.10 and above
- EOS:
  - 4.20.15M and above
  - 4.21.9M and above
  - 4.22.3F and above
  - 4.23.1F and above
- CVP: 2019.1.0 and above
- Wi-Fi: 8.8.1 and above

Vulnerability References

- https://github.com/Netflix/security-bulletins/blob/master/advisories/third-party/2019-002.md
- https://groups.google.com/forum/#!topic/grpc-io/oXVR5Bv009o - Additional gRPC issue discovered during Arista's testing efforts, and has since been fixed by Google

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