Date: March 23, 2020

Version: 1.0

Revision	Date	Changes
1.0	March 23, 2020	Initial Release

The CVE-IDs tracking this issue: CVE-2019-17596
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 a security vulnerability in an open-source software, Go. Arista has not received evidence of this vulnerability being exploited, as of the date of the initial release of this advisory.

The exploitation of this vulnerability on affected software can lead to panic upon an attempt to process network traffic containing an invalid DSA public key. There are several attack scenarios, such as traffic from a client to a server that verifies client certificates.

- **EOS** - In EOS, the exposure is limited to the state streaming components - TerminAttr and OpenConfig. 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. All other EOS components are not affected.
- **MOS (7130 Series)** - MOS is not affected by this CVE in its default configuration, nor is it affected if any configuration changes are made with MOS CLI commands.
- **CloudVision Portal** - The ingest component in the CVP Backend is affected via gRPC interfaces
- **Wi-Fi software** - This vulnerability does not impact Wi-Fi software components nor the Access Points using default configurations. The gRPC/gNMI interface can be manually enabled on Access Points. If the interface is manually enabled, admins should validate that the interface is only accessible via internal networks.

Symptoms

An attack due to this vulnerability would manifest in the form of a panic affecting the processing program, but not affecting other components of the product. This would occur when the product is provided an invalid public key to validate. The impact in EOS would be limited to the TerminAttr and OpenConfig agents, and an exploit like this can lead to Denial-of-Service (DoS).

Vulnerability Assessment

Affected Software

- TerminAttr:
    - All versions v1.7.2 and below

- CloudVision Portal (CVP):
  - 2019.1.0, 2019.1.1, 2019.1.2
  - All releases in the 2018 release train
- EOS
  - 4.23.1F and below
- MOS
  - 0.25 and below (While MOS is not vulnerable, it does use affected components in versions 0.25 and below)

Affected Software

This is a platform-independent vulnerability

Mitigation

As a security best practice, it is recommended to restrict public access to internal devices to safeguard from potential attacks. As a resolution against this vulnerability, refer to the next section for remediated software versions.

Resolution

This vulnerability is tracked using the following Bug IDs:

- BUG464752 is for EOS/OpenConfig
- BUG464753 is for TerminAttr
- BUG464757 is for CVP
- MOS-1092 for MOS

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 device operation or traffic forwarding, and addresses this vulnerability. During the TerminAttr update, the connection to the streaming endpoint (CVP or other tools) is reset and streaming telemetry is buffered until TerminAttr is running again and the connection is re-established. Arista recommends using CVP to upgrade TerminAttr across all devices. To identify the version of Terminattr in EOS, use the following commands:

```
switch#show version detail | grep TerminAttr-core
TerminAttr-core      v1.7.3          1
```

CloudVision - The vulnerability is addressed in 2019.1.3 and later versions of CloudVision Portal.

MOS - Upgrade to MOS 0.26 or later. While MOS is not vulnerable, it does use affected components that are fixed in version 0.26 or later.

The vulnerability is fixed in the following versions:

- TerminAttr:
  - v1.7.3 and later releases
- EOS/OpenConfig:
  - 4.23.2F and later releases
- CVP:
  - 2019.1.3 and later releases
- MOS:
  - 0.26 and later releases

Vulnerability References

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17596

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