Date: January 16th, 2019

Version: 1.0

Revision	Date	Changes
1.0	January 16th, 2019	Initial Release

The CVE-IDs tracking this issue are CVE-2018-16873, CVE-2018-16874 and CVE-2018-16875

Description

This advisory is to document the impact of CVE-2018-16873, CVE-2018-16874 and CVE-2018-16875 on EOS and CloudVision Portal. The listed CVEs track vulnerabilities identified in packages of the 'Go' programming language.

EOS features OpenConfig and the State Streaming agent 'TerminAttr' (EOS agent for streaming telemetry) are built using 'Go'.

CVE-2018-16873 (remote command execution during "go get -u") and CVE-2018-16874 (directory traversal in "go get") do not affect released versions of EOS, TerminAttr and CloudVision Portal.

CVE-2018-16875 specifically affects Go TLS servers accepting client certificates and TLS clients verifying certificates. The vulnerability could lead to a CPU denial of service attack in the certificate chain validation process. OpenConfig and TerminAttr gNMI servers running on EOS to enable state streaming are affected by CVE-2018-16875 only when configured to use client certificate authentication. The affected servers typically stream state information to telemetry collectors such as gRPC/gNMI telemetry collectors, Kafka and other collector infrastructures capable of ingesting streaming telemetry over gRPC/gNMI.

CloudVision Portal is not affected by CVE-2018-16875.

The following table shows affected EOS and TerminAttr versions

Bug IDs: 348164, 348165

Affected EOS versions:

EOS	TerminAttr
EOS-4.21.3F	1.5.2-1 1.5.0-1 1.4.1-1 1.3.1-1 1.1.1-1 0.19.x and older versions

Affected Platforms

OpenConfig and TerminAttr are platform independent features. All platforms are affected.

Symptoms

This vulnerability can be exploited only if OpenConfig or TerminAttr features are configured to use client certificates for authentication on affected software versions. On EOS devices configured to use OpenConfig/TerminAttr with client certificate based authentication, the following configuration will be present in the running-configuration. The configs in bold highlight the use of certificate chains for authentication in the two features.

```
OpenConfig:
!
management api gnmi
   transport grpc default
      ssl profile
    no shutdown
!
management security
   ssl profile
      trust certificate

TerminAttr:
!
daemon TerminAttr
   exec /usr/bin/TerminAttr -ingestgrpcurl= -taillogs -ingestauth=key, -certfile , -c
lientcafile
   no shutdown
```

Mitigation

It is recommended to disable certificate based authentication for affected features - OpenConfig and TerminAttr, and configure password based authentication as an interim workaround. Disabling certificate based authentication automatically defaults to password based authentication and no further configuration is required. Certificate authentication can be disabled in the SSL profile using the following commands:

```
OpenConfig
switch(config)#management security
switch(config-mgmt-security)# ssl profile test
switch(config-mgmt-sec-ssl-profile-test)#no trust certificate
```

```
TerminAttr:
!
daemon TerminAttr
   exec /usr/bin/TerminAttr -ingestgrpcurl= -taillogs -ingestauth=key,
no shutdown
```

Resolution:

Bugs 348164 and 348165 track this vulnerability for OpenConfig and TerminAttr, respectively. The fix for this issue will be available in the following software versions:

- For OpenConfig, the vulnerability will be addressed in EOS version 4.21.4F
- For state streaming using TerminAttr, the fix will be available in version 1.5.3 and later releases

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