**Updated: March 29th, 2021**

| Revision | Date | Changes |
|---|---|---|
| 1.0 | March 16th, 2021 | Initial Release |
| 1.1 | March 29th, 2021 | -Telegraf removed from affected EOS features<br>- Influxdb removed from affected components in MOS<br>- Added config for SSL profile with trust certificate configuration<br>- Added config check for vulnerable configuration in TerminAttr<br>- Updated assessment for CVP<br>- Updated mitigation for EOS, CVP and MOS |

The CVE-ID tracking this issue: CVE-2020-28362

CVSSv3.1 Base Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

## Description

This advisory documents the impact of a publicly disclosed vulnerability in the Go programming language (maintained by Google), on Arista products. Affected products include EOS, CloudVision Portal and MOS software. Affected features and software releases are listed in the sections below.

The vulnerability affects features that use TLS connections or client certificate authentication. When exploited, the vulnerability can allow denial of service attacks for the affected features.

- EOS devices running the affected releases are vulnerable if any of the following features are enabled.The impact is an agent crash for the affected feature.
    - TerminAttr - Used for streaming telemetry to Arista CloudVision.
    - gRIBI - Used to insert entries in the routing table from an external client.
    - Octa - Combines gNMI service support for OpenConfig and certain TerminAttr functionality.
    - OpenConfig - Used for the OpenConfig standard which allows for both streaming telemetry and configuration.

Copyright 2024 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.

- On 7130 systems running MOS, the Docker application may experience a crash. A Docker application crash does NOT impact the existing containers running on the system but it results in an application restart.
- CloudVision Portal is vulnerable as it uses TLS connections to connect to EOS devices. As the result of an exploit, the ingest component of the CVP backend may crash and affect overall product functionality.

Arista is not aware of any malicious uses of this issue in customer networks.

## Vulnerability Assessment

### Affected Software

**CloudVision Portal:**

- 2020.1.2 and below releases in the 2020.1.x train.
- 2020.2.4 and below releases in the 2020.2.x train.
- 2020.3.0 release

**EOS:**

- 4.25.0F
- 4.25.1F (if gRIBI is configured).

**TerminAttr:**

- TerminAttr-v1.11.0
- TerminAttr-v1.11.1
- TerminAttr-v1.12.0

**MOS:**

- MOS-0.28.4 and below releases in the MOS-0.28.x train.
- MOS-0.29.0
- MOS-0.30.0

## Affected Platforms

- The following products are affected by this vulnerability:
    - 7010 series
    - 7020R Series
    - 7130 series
    - 7150 series
    - 7280E/R/R2 series
    - 7280R3/ 7500R3 / 7800R3 series

Copyright 2024 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.

  - 7500E/R/R2 series
  - 7050X/X2/X3 series
  - 7060X/X2/X4 series
  - 7160 series
  - 7170 series
  - 720X series
  - 7250X/7250X2 series
  - 7260X/X3 series
  - 7300X/X3 series
  - 7320X series
  - 7368X4 series
  - CloudVision Portal, virtual appliance or physical appliance
  - CloudEOS Virtual Router, as a VM on-premises or in the public cloud marketplaces
  - CloudEOS Container, that runs in Kubernetes on-premises clusters

- The following products are **not** affected:
  - Arista Converged Cloud Fabric and DANZ Monitoring Fabric (Formerly Big Switch Nodes for BCF and BMF)
  - Arista Wireless Access Points
  - Awake Security Solutions
  - CloudVision eXchange
  - CloudVision Wi-Fi (on-premise and cloud service delivery)
  - CloudVision as a Service

## Symptoms

### I) Vulnerable Configuration

### 1) On systems running EOS:

**a) For gRIBI, Octa and OpenConfig:**
For the first step, confirm if there is any SSL profile present in the running-configuration with client certificate authentication enabled:

```
Switch#show running-config section management security
management security
   ssl profile test
      trust certificate certificate_name
```

In the above example, a SSL profile “test” has been configured. The “trust certificate certificate_name” piece of configuration indicates that client certificate authentication is enabled

Copyright 2024 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.

in the profile.

Next, confirm if any of the SSL profiles with client certificate authentication enabled have been applied to the following features:

(i) Confirm if gRIBI has been configured along with a SSL profile.

```
Switch#show management api gribi
Enabled:                Yes
Server:                 running on port 6040
SSL Profile:            test
```

If yes, confirm that the SSL profile has client certificate authentication enabled.

(ii) Or confirm if management api gnmi has been configured along with a SSL profile with client certificate authentication enabled:

```
Switch#show management api gnmi
Enabled:            Yes
Server:             running on port 50051, in default VRF
SSL Profile:        test
QoS DSCP:           none
```

If yes, confirm that the SSL profile has client certificate authentication enabled.

Note: Step (ii) covers the check for both Octa and OpenConfig.

**b) For TerminAttr**

For the first step, confirm if TerminAttr is running:

```
Switch#show daemon TerminAttr
Process: TerminAttr (running with PID 4060)
Uptime: 2 days, 3:48:28 (Start time: Sun Jan 31 06:00:43 2021)
No configuration options stored.
```

Copyright 2024 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.

```
```

Note: The TerminAttr Process ID (PID) will differ from what is highlighted in the above example.

If TerminAttr is running, the corresponding version can be checked via the following

```
Switch#show version detail | grep TerminAttr-core
TerminAttr-core      v1.12.0         1
```

Once the TerminAttr version has been checked, the following steps can be followed to determine if the system is vulnerable:

i) Confirm that the TerminAttr daemon configuration has the “-grpcaddr” and “-clientcafile” flags configured:

```
Switch#show running-config section TerminAttr
daemon TerminAttr
exec /usr/bin/TerminAt
tr --disableaaa -taillogs -grpcaddr=test/0.0.0.0:6042
-allowed_ips=0.0.0.0/0 -procfsperiod=60s -cpu_counters_expiration=60
-clientcafile=path_to_certificate
no shutdown
```

The presence of these flags indicate that client certificate authentication has been enabled for TerminAttr.

ii) Or confirm that the “-cvaddr” or “-ingestaddr” flags are configured. If yes, verify that the “-cvauth” or “-ingestauth” flags are NOT set to “none”:

Copyright 2024 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.

```
Switch#show running-config section TerminAttr
daemon TerminAttr
exec /mnt/flash/TerminAttr
-cvaddr=10.10.10.100:443 -cvcompression=gzip -taillogs
-grpcaddr 0.0.0.0:6042 --autocert=true
--cvauth=certs
,/persist/secure/cloudvision/enroll.crt,/persist/secure/cloudvision/pr
ivate.pem
no shutdown
```

In this example, the “-cvaddr” flag is configured and the “--cvauth” flag is NOT set to none.

**2) On CloudVision Portal Servers:**

Confirm if the version of CVP running is among the list of affected versions mentioned in the “Affected Software” section:

- Login to the CVP server
- Navigate to /cv/settings/general
- Confirm the version of CVP running:




As seen in the above example, 2020.2.4 is the CVP version running on the server and is included in the list of CVP versions to which the vulnerability is applicable.

Copyright 2024 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.

### 3) On 7130 systems running MOS:

Confirm if a docker container has been configured via “**show running-configuration”:**

Example:

```
docker container foo run image registry.example.com/busybox:latest
```

### II) Determining if the vulnerability has been hit:

If the vulnerability has been exploited, the following crash log may be observed on affected products:

```
panic: impossible [recovered]
       panic: impossible
goroutine 195 [running]:
       runtime/panic.go:969 +0x1b9
math
 /big.nat.divRecursiveStep(0xc0000da400, 0x39, 0x3d, 0xc000091080, 0xa
8, 0xad, 0xc00064c000, 0x70, 0x7534, 0x0, ...)
       math /big/nat.go:951 +0x139a
math/big.nat.divRecursive(0xc0000da400, 0x39, 0x3d, 0xc000091080, 0xa9
, 0xad, 0xc00064c000, 0x70, 0x7534)
       math /big/nat.go:828 +0x17e
math/big.nat.divLarge(0xc000264000, 0x10, 0x14, 0xc000264000, 0x10, 0x
14, 0xc000090b00, 0xa8, 0xab, 0xc00011b000, ...)
       math /big/nat.go:727 +0x412
math/big.nat.div(0xc000264000, 0x10, 0x14, 0xc000264000, 0x10, 0x14, 0
xc000090b00, 0xa8, 0xab, 0xc00011b000, ...)
       math /big/nat.go:672 +0x410
```

Figure-1: Stack trace

Note that the stack trace may vary from case to case, however if the highlighted portion of the trace (i.e. “math”) is present, it is a strong indicator that the vulnerability has been hit. The following steps list the commands that can be used to identify the crash log on the affected products.

Copyright 2024 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.

**1) On systems running EOS:**

An EOS agent crash may be observed as a result of an exploit. To identify agent crashes, navigate to the /var/log/agents directory in the bash shell and individually view the following agent logs by running "**cat agent_name-PID**". The relevant agent names are as follows:

- TerminAttr-PID
- Octa-PID
- OpenConfig-PID
- gRIBI-PID

An example of how the agent log can be viewed is as follows:

"**cat TerminAttr-3553**"

In this example, 3553 is the PID (Process Identifier).

-OR-

Run "**show agent logs crash**" in the CLI. The output of this command should have sections of the logs shown in Figure-1 above highlighted in yellow.

**2) On CloudVision Portal Servers (via the CLI shell):**

(i) Execute "**cat /cvpi/apps/aeris/logs/ingest.stderr.log**"

(ii) Execute "**cat /cvpi/apps/aeris/logs/api-server.stderr.log**"

Note: For CVP clusters, perform the above check on all 3 nodes.

The output of this command should have sections of the logs shown in Figure-1 above highlighted in yellow.

**3) On 7130 systems running MOS:**

Execute "**journalctl -u docker.service**"

The output of this command should have sections of the logs shown in Figure-1 above highlighted in yellow.

Copyright 2024 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.

## Mitigation

As a security best practice, TLS connections should only be accepted from trusted sources. The following options are available to restrict incoming TLS connections:

**1) On systems running EOS:**

Configure a non-default Control-Plane ACL with the following rule present:

**permit tcp 10.10.10.0/24 any eq 443**

In this example, HTTPs connections (i.e. connections to port 443) will only be accepted if sourced from the 10.10.10.0/24 subnet. The following are the default service ports for the affected features:

(i) gRIBI - 6040
(ii) OpenConfig and Octa - 6030
(iii) TerminAttr - 6042

The relevant service ports will need to be specified in the ACL rule.

Note:
i) If a different TCP port is used on the Switch for the incoming TLS connection from what is referenced above, modify the port number in the ACL rule.

ii) For TerminAttr, ensure that the connection to Cloudvision is established over a trusted network.

**2) On CloudVison Portal servers (via the CLI shell):**

Configure the following iptable rules on the CVP server(s) to permit incoming TCP connections to ports 9910 and 8443 from a specified subnet only:

```
sudo iptables -A INPUT -p tcp -s 10.10.10.0/24 --dport 9910 -m conntra
ck --ctstate NEW,ESTABLISHED -j ACCEPT
```

Copyright 2024 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.

```
sudo iptables -A INPUT -p tcp -s 10.10.10.0/24 --dport 8443 -m conntra
ck --ctstate NEW,ESTABLISHED -j ACCEPT
```

In this example, TCP connections to ports 9910 and 8443 will be accepted only if sourced from the 10.10.10.0/24 subnet.

Note:
These iptable rules are not persistent across reboots and must be applied on a reboot of the system.

**3) On 7130 systems running MOS:**

There is no workaround available to mitigate the issue on 7130 systems running MOS. As a security best practice, ensure that TLS connections are made to trusted devices.

For the final resolution, please refer to the next section which lists the details of the remediated software versions.

## Resolution

The recommended resolution is to upgrade to a remediated software release during a maintenance window. This vulnerability is tracked by the following BUGs:

**1) EOS**

- TerminAttr
  - The vulnerability in EOS systems running TerminAttr is tracked by BUG538523.
  - Fixed in TerminAttr-v1.12.1
- OpenConfig/Octa
  - The vulnerability in EOS systems running OpenConfig and Octa is tracked by BUG538500.
  - Fixed in EOS-4.25.1
- gRIBI
  - The vulnerability in EOS systems running gRIBI is tracked by BUG539212.
  - Fixed in EOS-4.25.2

Copyright 2024 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.

### 2) CloudVision Portal

The vulnerability in CVP is tracked by BUG541154 and the fix will be available in the following releases:

- 2020.3.1
- 2021.1.0

### 3) MOS

The vulnerability in systems running MOS is tracked by BUG MOS-1729. This has been fixed in the following release:

- MOS-0.30.1

### For More Information

To read more about this vulnerability, please refer to the following links:

- MITRE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28362
- Google Groups: https://groups.google.com/g/golang-nuts/c/c-ssaaS7RMI

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 2024 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.