Date: January 11th, 2022

Revision	Date	Changes
1.0	January 11th, 2022	Initial release

Security Advisory 0071

The CVE-ID tracking this issue: CVE-2021-28500
CVSSv3.1 Base Score: 9.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H)

The CVE-ID tracking this issue: CVE-2021-28501
CVSSv3.1 Base Score: 9.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H)

The CVE-ID tracking this issue: CVE-2021-28506
CVSSv3.1 Base Score: 9.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H)

The CVE-ID tracking this issue: CVE-2021-28507
CVSSv3.1 Base Score: 5.5 (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:H/A:N)

Description

This advisory documents the impact of several vulnerabilities related to OpenConfig transport protocols in Arista's EOS software. Affected software releases are listed below.

CVE-2021-28500, CVE-2021-28501 - An issue has recently been discovered where the incorrect use of EOS's AAA API's by the OpenConfig and TerminAttr agents could result in unrestricted access to the device for local users with nopassword configuration.

CVE-2021-28506 - Certain gNOI APIs incorrectly skip authorization and authentication which could potentially allow a factory reset of the device.

CVE-2021-28507 - Under certain conditions, the service ACL configured for OpenConfig gNOI and OpenConfig RESTCONF might be bypassed, which results in the denied requests being forwarded to the agent.

Acknowledgements

Arista would like to acknowledge and thank Miles Sutcliffe @ https://sutcliffe.it/ for responsibly reporting CVE-2021-28500
CVE-2021-28501, CVE-2021-28506 and CVE-2021-28507 were found internally at Arista on Arista devices.

None of the vulnerabilities are known to be actively used maliciously in the field.

Vulnerability Assessment

Affected Software

CVE-2021-28500

- 4.26.1F and below releases in the 4.26.x train
- 4.25.4M and below releases in the 4.25.x train
- 4.24.6M and below releases in the 4.24.x train
- 4.23.8M and below releases in the 4.23.x train
- 4.22.11M and below in 4.22.x train
- 4.21.14M and below in 4.21.x train
- All prior releases

CVE-2021-28501

- TerminAttr v1.16.1 and all prior releases

CVE-2021-28506

- 4.26.2F and below releases in the 4.26.x train
- 4.25.5.1M and below releases in the 4.25.5.x train
- 4.25.4M and below in the 4.25.4.x train
- All prior releases in 4.25.x train
- 4.24.7M and below to 4.24.2F in the 4.24.x train

CVE-2021-28507

- 4.26.2F and below releases in the 4.26.x train
- 4.25.5.1M and below releases in the 4.25.5.x train
- 4.25.4M and below in the 4.25.4.x train
- All prior releases in 4.25.x train
- 4.24.7M and below releases in the 4.24.x train
- 4.23.9M and below releases in the 4.23.x train
- All releases in 4.22.x train
- All releases in 4.21.x train
- All prior releases

Affected Platforms

This is a platform-independent vulnerability and affects all systems running EOS with the versions identified above.

The following product versions and platforms are not affected by this vulnerability:

- Arista Wireless Access Points

- CloudVision WiFi, virtual appliance or physical appliance
- CloudVision WiFi 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)
- Awake Security Platform

Required Configuration for Exploitation

Configuration vulnerable to CVE-2021-28500

OpenConfig gNMI/gNOI is enabled, or

```
management api gnmi
   transport grpc default
```

OpenConfig RESTCONF is enabled

```
management api restconf
   transport https default
```

and no password remote login authentication is disabled

```
no aaa authentication policy local allow-nopassword-remote-login
```

and a local user exists whose authentication is with nopassword.

```
username admin privilege 1 role network-admin nopassword
```

Configuration vulnerable to CVE-2021-28501

TerminAttr gNMI is enabled

```
daemon TerminAttr
   exec /usr/bin/TerminAttr ...
   no shutdown
```

and no password remote login authentication is disabled

```
no aaa authentication policy local allow-nopassword-remote-login
```

and a local user exists whose authentication is with nopassword.

```
username admin privilege 1 role network-admin nopassword
```

Configuration vulnerable to CVE-2021-28506

OpenConfig gNMI/gNOI

```
management api gnmi
   transport grpc default
```

Configuration vulnerable to CVE-2021-28507

A service ACL is configured and

```
ip access-list standard oc-acl
   10 permit host 10.1.1.1
   20 permit host 172.16.1.1/24
   30 deny any
```

gNMI/gNOI is configured with service ACL, or

```
management api gnmi
   transport grpc default
      ip access-group oc-acl
```

RESTCONF configured with service ACL.

```
management api restconf
   transport https default
      ip access-group oc-acl
```

Notes

Mutual TLS

If a mutual TLS certificate is configured for gNMI or TerminAttr, the server may not be affected by authentication vulnerabilities CVE-2021-28500, CVE-2021-28501 and CVE-2021-28506. This does not apply to RESTCONF.

OpenConfig gNMI is configured with SSL profile

```
management api gnmi
   transport grpc default
      ssl profile mtls-grpc-profile
management security
   ssl profile mtls-grpc-profile
      certificate target.crt key target.key
      trust certificate ca.crt
```

TerminAttr is configured with SSL profile

```
daemon TerminAttr
   exec /usr/bin/TerminAttr
      -certfile /persist/secure/ssl/certs/target.crt
      -keyfile /persist/secure/ssl/keys/target.key
      -clientcafile /persist/secure/ssl/certs/ca.crt
   no shutdown
```

Symptoms

The following system logs at /var/log/messages may indicate vulnerability to CVE-2021-28500. When a gNMI Set is issued, the host should be recognized.

```
Nov 24 02:31:20 cd217 ConfigAgent: %SYS-5-CONFIG_SESSION_ENTERED: User
 ad
min en
tered config
uration session session1068691224937 on GNMI (10.24.128.7:46054)
Nov 24 02:31:22 cd217 ConfigAgent: %SYS-5-CONFIG_SESSION_COMMIT_SUCCES
S: User admin committed configuration session session1068691224937 suc
cessfully on GNMI (10.24.128.7:46054)
Nov 24 02:31:22 cd217 ConfigAgent: %SYS-5-CONFIG_SESSION_EXITED: User
```

```
admin exited configuration session session1068691224937 on GNMI (10.24
.128.7:46054)
```

The following symptoms may indicate vulnerability to this issue:

Check if the installed software is an affected version.
Terminattr

```
switch#show version detail | grep TerminAttr-core
TerminAttr-core      v1.15.3          1
```

Mitigation

The following configuration changes may be made in order to remedy the exploitation of the listed vulnerabilities.

Disable affected agents:

On the affected versions, all vulnerabilities can be mitigated by disabling OpenConfig gNMI/gNOI and OpenConfig RESTCONF and TerminAttr. If use of these agents is required, a hotfix employing a proxy service can be deployed.

Disable OpenConfig gNMI

```
management api gnmi
   transport grpc default
      shutdown
```

Disable OpenConfig RESTCONF

```
management api restconf
   transport https default
      shutdown
```

Disable OpenConfig TerminAttr

```
daemon TerminAttr
    shutdown
```

CVE-2021-28500 and CVE-2021-28501

For local users whose authentication is with nopassword, enforce a password or remove the user.

Ensure that the following configuration does not exist where a local user is configured with nopassword.

```
username admin nopassword
```

Instead, a password can be enforced for the local user.

```
username admin secret 0 pass123
```

Please refer to the EOS user security manual for further information.

CVE-2021-28506 and CVE-2021-28507

No mitigation options available

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

Resolution

The vulnerabilities listed below, as identified by their CVE numbers, are being tracked by the following bugs:

CVE-2021-28500 - BUG 601875
CVE-2021-28501 - BUG 604880
CVE-2021-28506 - BUG 606192
CVE-2021-28507 - BUG 606248

The recommended resolution is to upgrade to a remediated software version at your earliest convenience. Arista recommends customers move to the latest version of each release that contains all the fixes listed below.

CVE-2021-28500 has been fixed in the following releases:

- 4.26.2F and later releases in the 4.26.x train

- 4.25.5M and later releases in the 4.25.x train
- 4.25.4.1M and later releases in the 4.25.4.x train
- 4.24.7M and later releases in the 4.24.x train
- 4.23.9M and later releases in the 4.23.x train
- 4.22.12M and later releases in the 4.22.x train
- 4.21.15M and later releases in the 4.21.x train

CVE-2021-28501 has been fixed in the following releases:

- TerminAttr v1.16.2 and later releases

CVE-2021-28506 has been fixed in the following releases:

- 4.26.3M and later releases in the 4.26.x train
- 4.25.6M and later releases in the 4.25.x train
- 4.25.4.1M and later releases in the 4.25.4.x train
- 4.24.8M and later releases in the 4.24.x train

CVE-2021-28507 has been fixed in the following releases:

- 4.26.3M and later releases in the 4.26.x train
- 4.25.6M and later releases in the 4.25.x train
- 4.25.4.1M and later releases in the 4.25.4.x train
- 4.24.8M and later releases in the 4.24.x train
- 4.23.10M and later releases in the 4.23.x train

For immediate remediation until EOS can be upgraded, the following hotfix is available.

Hotfix

To mitigate CVE-2021-28500, CVE-2021-28501, CVE-2021-28506 and CVE-2021-28507 with the continued use of the affected agents, a hotfix employing a proxy service can be deployed. The proxy is configured behind the gNMI/gNOI or RESTCONF server.

OpenConfigProxy is a universal proxy for the OpenConfig gNMI/gNOI server, OpenConfig RESTCONF server or TerminAttr gNMI server. The proxy performs:

- IP ACL check
- Authentication
- Authorization (for gNMI/gNOI only, disabled by default)

Requests are forwarded to the OpenConfig gNMI/gNOI server or RESTCONF server or TerminAttr gNMI server. Responses are sent to the collector from the gNMI/gNOI server or RESTCONF server via the proxy.

Hotfix Notes:

- The hotfix employing a proxy service is version agnostic (i.e., the proxy can be installed on any affected version).
- The hotfix employing a proxy service does not require a restart of the OpenConfig/Octa agent. Only OpenConfig gNMI or RESTCONF configuration changes are required.
- The hotfix employing a proxy service installation is hitless and a reload of the switch is not required for the hotfix to take effect.

TerminAttr Note: For TerminAttr, it is recommended to update to TerminAttr v1.16.3 or above as its agent can be updated independently of the EOS version.

The following hotfix is available to remedy all CVE's listed in this Security Advisory:

32 bit platform:
Version: 1.0
URL: OpenConfigProxy.i386.swix
SWIX hash: (SHA-512)
fef14efde0ba282ab90664ffbd5ff6d37172062ea5f97fc44b457d0b0922d4c7bc5780a0d0f89dbe540fd38e3daa875b46b5f7d57edb3973212d8b2f7f1ec7d6

64 bit platform:
Version: 1.0
URL: OpenConfigProxy.x86_64.swix
SWIX hash: (SHA-512)
db4488cb6328fb93bdcbcc11edfff95be92755b5acc263d0ecff70c879e52fe51471eb1783acb9dc53a9115f575dc7146b8984c26d4282806b37b0dc5ded18c2

For detailed information on installation and configuration of the OpenConfigProxy please refer to the documentation here

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:

Please visit Customer Support for up to date information on how to open a service request via email or telephone.