Date: January 11th, 2022

To resolve CVE-2021-28500, CVE-2021-28506 and CVE-2021-28507 with the continued use of OpenConfig, an OpenConfigProxy hotfix can be deployed. The proxy is configured behind the OpenConfig gNMI/gNOI or RESTCONF server.

OpenConfigProxy is a universal proxy for the OpenConfig gNMI/gNOI server or OpenConfig RESTCONF 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. Responses are sent to the collector from the gNMI/gNOI server or RESTCONF server via the proxy.

Notes:

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

For instructions on installation and verification of the hotfix patch, refer to the "managing EOS extensions" section in the EOS User Manual. Ensure that the patch is made persistent across reboots by running the command `copy installed-extensions boot-extensions`.

```
switch#bash OpenConfigProxy --help
Usage of OpenConfigProxy:
  -allowed_ips value
      Comma-separated list of allowed IPv4/IPv6 client addresses of form IP
address/mask. If no addresses are specified, any IPv4/IPv6 address is
permitted.
  -authorization
      Enable authorization. Only applicable to gNMI/gNOI. By default,
authorization is not performed.
  -destination_port int
      Port that the destination gNMI/RESTCONF server listens on (1-65535).
Must be specified.
  -destination_ssl
      A TLS/SSL connection is used by the proxy client for dialing the
destination. Applicable only to the gNMI proxy. A RESTCONF proxy client
always uses a TLS/SSL connection.
```

Copyright 2022 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.

```
  -destination_ssl_profile string
      TLS/SSL profile name used by the proxy client for dialing the
destination.
  -destination_vrf string
      VRF that the proxy client dials from. If not specified, uses the VRF
specified by -vrf.
  -dscp int
      DSCP value for the proxy server (0-63).
  -gnmi
      Enable the gNMI/gNOI proxy server.
  -log_backtrace_at value
      when logging hits line file:N, emit a stack trace
  -port int
      Port that the proxy server listens on (1-65535). Must be specified.
  -restconf
      Enable the RESTCONF proxy server.
  -ssl_profile string
      TLS/SSL profile name certificate used by the proxy server. Must be
specified for the RESTCONF proxy server.
  -ssl_profile_ca string
      TLS/SSL profile name CA certificate used by the proxy server.
  -v value
      log level for V logs
  -vevent value
      comma-separated list of pattern=N settings for file name or EOS path
filtered logging (file name based on location of the mapper)
  -vmodule value
      comma-separated list of pattern=N settings for file-filtered logging
  -vrf string
      VRF to listen in for the proxy server. (default "default")
```

gNMI/gNOI Proxy

An OpenConfigProxy daemon will be configured. The following gNMI CLI configuration can be translated to the following proxy daemon arguments.

original CLI configuration	OpenConfigProxy daemon argument
`management api gnmi` `  transport grpc TRANSPORT_NAME`	`-gnmi`

`management api gnmi`
`  provider eos-native`
`  transport grpc TRANSPORT_NAME`
	`-gnmi`

`  vrf VRF_NAME`	`-vrf VRF_NAME`
`  port PORT_NUMBER`	`-port PORT_NUMBER`

Copyright 2022 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.

ssl profile PROFILE_NAME	-ssl_profile PROFILE_NAME
authorization requests	-authorization
qos dscp DSCP_VALUE	-dscp DSCP_VALUE
ip access-group ACL_NAME	-allowed_ips ALLOWED_IPS

OpenConfigProxy daemon CLI configuration

```
daemon OpenConfigProxy
   exec /usr/bin/OpenConfigProxy -gnmi ARGUMENT...
   no shutdown
```

Example

Original configuration

```
management api gnmi
   transport grpc default
      vrf mgmt
      port 9339
      ssl profile grpc-profile
      qos dscp 1
      authorization requests
      ip access-group grpc-acl
!
ip access-list standard grpc-acl
   10 permit host 10.1.1.1
   20 permit host 172.16.1.1/24
   30 deny any
!
management security
   ssl profile grpc-profile
      certificate target.crt key target.key
```

Configuration using the proxy

```
management api gnmi
   transport grpc default
      vrf mgmt
      port 49152
!
daemon OpenConfigProxy
   exec /usr/bin/OpenConfigProxy
      -gnmi
      -vrf mgmt
```

Copyright 2022 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.

```
      -port 9339
      -ssl_profile grpc-profile
      -dscp 1
      -authorization
      -allowed_ips 10.1.1.1/32,172.16.1.1/24
      -destination_port 49152
   no shutdown
```

Output of `show agent OpenConfigProxy logs`

```
I1123 07:09:54.101537    6056 main.go:333] gNMI/gNOI proxy server listening
on [::]:6030 in mgmt VRF using TLS/SSL profile "grpc-profile"
I1123 07:09:54.101573    6056 main.go:335] forwarding requests to
OpenConfig gNMI/gNOI server listening on localhost:49152 in mgmt VRF
```

The proxy listens on port 9339 in the mgmt VRF with the same gNMI server configuration as the original.

Configuration

- The OpenConfig gNMI server port needs to be changed to an intermediary port which can only be accessed locally. This would be a port blocked by the control plane ACL. The proxy dials to the OpenConfig gNMI server on this port with `-destination_port`. In the example, this was changed to 49152.
- The VRF of the proxy corresponds to the same VRF of the OpenConfig gNMI server. If the `-vrf` flag is not specified, the VRF of the proxy server defaults to the default VRF. A `-destination_vrf` flag can also be specified to allow the proxy to dial from a VRF different from its listening VRF.
- The DSCP value and authorization configuration of the OpenConfig gNMI server can be unconfigured because this is handled by the proxy server with arguments `-dscp` and `-authorization`.
- In the example, traffic is encrypted between the proxy and collector as the proxy gRPC server is configured with an TLS/SSL certificate.
- Traffic between the proxy and OpenConfig gNMI server is local and can remain encrypted or unencrypted. It is possible to use a TLS/SSL connection for the client proxy using `-destination_ssl`. It is also possible to pass a client certificate to the proxy using the `-destination_ssl_profile` argument, which uses the TLS/SSL certificate to dial to the local OpenConfig gNMI server. This encrypts the traffic between the proxy and OpenConfig gNMI server.
- By default, if no allowed IPs are specified via the `-allowed_ips` argument, all IPs are permitted. For the `-allowed_ips` argument, allowed IPs correspond to the service ACL configuration.

Copyright 2022 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.

- Verbose logging can be enabled with `-v 1`. This logs access attempts and RPCs issued, as well as gRPC debugging information.
- Proxy logs can be accessed with `show agent OpenConfigProxy logs`.

Limitations

- Any configuration changes to the proxy requires modifying the arguments and restarting the proxy daemon.
- If the TLS certificate is changed or rotated, the proxy daemon must be restarted using `shutdown/no shutdown`.

Authorization

If authorization is enabled for the proxy with `-authorization`, all gNMI and gNOI RPCs correspond to an OpenConfig.Get or OpenConfig.Set authorization command. In the affected releases, authorization is only supported for gNMI and not for gNOI.

gNMI/gNOI RPC	authorization command
`/gnmi.gNMI/Capabilities`	`OpenConfig.Get`
`/gnmi.gNMI/Get`	`OpenConfig.Get`
`/gnmi.gNMI/Set`	`OpenConfig.Set`
`/gnmi.gNMI/Subscribe`	`OpenConfig.Get`
`/gnoi.factory_reset.FactoryReset/Start`	`OpenConfig.Set`
`/gnoi.os.OS/Install`	`OpenConfig.Set`
`/gnoi.os.OS/Activate`	`OpenConfig.Set`
`/gnoi.os.OS/Verify`	`OpenConfig.Get`
`/gnoi.certificate.CertificateManagement/Rotate`	`OpenConfig.Set`
`/gnoi.certificate.CertificateManagement/GetCertificates`	`OpenConfig.Get`
`/gnoi.certificate.CertificateManagement/CanGenerateCSR`	`OpenConfig.Get`
`/gnoi.system.System/Ping`	`OpenConfig.Get`
`/gnoi.system.System/Traceroute`	`OpenConfig.Get`

Copyright 2022 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.

RESTCONF Proxy

An OpenConfigProxy daemon will be configured similarly to the gNMI/gNOI proxy. The following RESTCONF CLI configuration can be translated to the following proxy daemon arguments.

original CLI configuration	OpenConfigProxy daemon argument

`management api restconf`
`  transport https`
`TRANSPORT_NAME`
	`-restconf`

`management api restconf`
`  provider eos-native`
`  transport https`
`TRANSPORT_NAME`
	`-restconf`

`vrf VRF_NAME`	`-vrf VRF_NAME`
`port PORT_NUMBER`	`-port PORT_NUMBER`
`ssl profile PROFILE_NAME`	`-ssl_profile PROFILE_NAME`
`qos dscp DSCP_VALUE`	`-dscp DSCP_VALUE`
`ip access-group ACL_NAME`	`-allowed_ips ALLOWED_IPS`

OpenConfigProxy daemon CLI configuration

`daemon OpenConfigProxy`
`  exec /usr/bin/OpenConfigProxy -restconf ARGUMENT...`
`  no shutdown`

Example

Original configuration

```
management api restconf
   transport https default
      vrf mgmt
      port 6200
      ssl profile restconf-profile
      qos dscp 1
      ip access-group restconf-acl
!
ip access-list standard restconf-acl
   10 permit host 10.1.1.1
```

Copyright 2022 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.

```
   20 permit host 172.16.1.1/24
   30 deny any
!
management security
   ssl profile restconf-profile
      certificate target.crt key target.key
```

Configuration using the proxy

```
management api restconf
   transport https default
      vrf mgmt
      port 49152
      ssl profile restconf-profile
!
daemon OpenConfigProxy
   exec /usr/bin/OpenConfigProxy
      -restconf
      -vrf mgmt
      -port 6200
      -ssl_profile restconf-profile
      -dscp 1
      -allowed_ips 10.1.1.1/32,172.16.1.1/24
      -destination_port 49152
   no shutdown
```

Output of `show agent OpenConfigProxy logs`

```
I1123 08:47:14.343153   11275 main.go:385] RESTCONF proxy server listening
on [::]:6200 in mgmt VRF using TLS/SSL profile "restconf-profile"
I1123 08:47:14.343181   11275 main.go:387] forwarding requests to
OpenConfig RESTCONF server listening on https://localhost:49152 in mgmt VRF
```

The proxy listens on port 6200 in the mgmt VRF with the same RESTCONF server configuration as the original.

Limitations

- As with the gNMI/gNOI proxy, any configuration changes to the proxy requires modifying the arguments and restarting the proxy daemon.
- If the TLS certificate is changed or rotated, the proxy daemon must be restarted using `shutdown/no shutdown`.
- As with the RESTCONF server, the RESTCONF proxy server must be configured with an SSL profile.

Copyright 2022 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.

Multiple proxies

If multiple gNMI servers are configured or if there is a gNMI server and a RESTCONF server is configured, then multiple proxy daemons can be configured.

```
daemon OpenConfigProxyGNMI
   exec /usr/bin/OpenConfigProxy -gnmi ...
   no shutdown
!
daemon OpenConfigProxyRESTCONF
   exec /usr/bin/OpenConfigProxy -restconf ...
   no shutdown
```

Copyright 2022 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.