Cisco IOS XR Resilient Infrastructure

Contents

Introduction

This document describes one hardening aspect of Cisco IOS$^{®}$ XR: phase out insecure features and ciphers systematically.

Cisco IOS XR Resilient Infrastructure

To increase the security posture of Cisco devices, Cisco is making changes to default settings, deprecating and eventually removing insecure capabilities, and introducing new security features. These changes are designed to strengthen your network infrastructure and provide better visibility into threat actor activities.

Do look at this Trust Center page: Resilient Infrastructure. It mentions the Infrastructure Hardening, the Cisco IOS XR Software Hardening Guide, the Feature Deprecation process, and Feature Deprecation and Removal Details. The suggested alternatives are mentioned here: Feature removal and Suggested Alternatives.

Cisco IOS XR is phasing out insecure features and ciphers. This includes both configuration and execute commands in Cisco IOS XR.

Impacted Features

- Telnet
- TFTP
- FTP
- HTTP
- SNMP v1/v2c
- SNMP v3 without authPriv
- IP Source Route
- TCP/UDP Small Servers
- TACACS+ and Radius with pre-shared keys (Type 7) and MD5
- SSH v1
- TLS 1.0/1.1
- NTPv2/3 and MD5
- GRPC no TLS, TLSv1.0/1.1
- Exec commands using copy, utility, and install with TFTP/FTP

Grouping

There are configuration commands, but also execute commands (for example the "copy" command).

The deprecated commands can be grouped:

- SSHv1, Telnet (server and client), TFTP (client), FTP
- DSA host-key, TACACS/RADIUS Type 7, TLS 1.0/1.1
- Other: TCP/UDP small servers, IP source routing (IPv4 and IPv6)

Phases

This project follows the usual feature deprecation approach: warn -> restrict -> remove.

- Warnings in Cisco IOS XR release 25.4.1.
- Restriction phase
- Feature removal

Warning Phase

What are the warnings?

1. The CLI (Command Line Interface) help function
2. A syslog warning
3. A description warning in the yang module

Warnings are emitted for configured insecure options. These are syslog messages with a**frequency of 30 days**.

When any insecure feature is used, this log warning (level 4 or warning) is emitted:

***%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN**: Feature '<feature-name>' utilised or configured. This feature is known to be insecure, consider ceasing use of this feature. <Recommendation>*

The recommendation is what to use instead of the insecure option.

Example warning for FTP :

%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Feature 'FTP' utilised or configured. This feature is known to be insecure, consider ceasing use of this feature. Recommend to use SFTP.

Notice the words utilised or configured. Utilised refers to an execute command and configured refers to a configuration command.

A warning message can be printed if the insecure option is removed (level 6 or informational). Example:

RP/0/RP0/CPU0:Oct 22 06:43:43.967 UTC: tacacsd[1155]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED : Insecure feature 'TACACS+ over TCP with shared secret (default mode)' configuration removed.

List of Deprecated Insecure Options

This is the list of insecure options that trigger a warning in Cisco IOS XR releases of the warning phase.

The list shows the insecure option, the configuration or execute commands, the warning message, and associated Yang model.

IP source routing (RFC 791)

CLI

```
<#root>
RP/0/RP0/CPU0:Router(config)#
ip ?

  source-route       Process packets with source routing header options (This is deprecated sin
RP/0/RP0/CPU0:Router(config)#
ipv4 ?

  source-route     Process packets with source routing header options (This is deprecated since
RP/0/RP0/CPU0:Router(config)#
ipv6 ?

  source-route     Process packets with source routing header options (This is deprecated since
```

ip source route

ipv6 source-route

ipv4 source-route

Warning

RP/0/RP0/CPU0:Oct 17 19:01:48.806 UTC: ipv4_ma[254]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Feature 'IPV4 SOURCE ROUTE' utilized or configured. This feature is known to be insecure, consider ceasing use of this feature. Do not enable IPv4 Source

Routing due to security risks.

RP/0/RP0/CPU0:Oct 17 19:01:48.806 UTC: ipv6_io[310]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Feature 'IPV6 SOURCE ROUTE' utilized or configured. This feature is known to be insecure, consider ceasing use of this feature. Do not enable IPv6 Source Routing due to security risks.

Yang Model

Cisco-IOS-XR-ipv4-ma-cfg

Cisco-IOS-XR-ipv6-io-cfg

Cisco-IOS-XR-um-ipv4-cfg

Cisco-IOS-XR-um-ipv6-cfg

Recommendation

Remove the insecure option.

No exact alternative exists. Customers wanting to control traffic through a network based on source address can do so using policy-based routing or other administrator controlled source routing mechanisms that do not leave the routing decision to the end user.

SSH v1

CLI

```
<#root>
RP/0/RP0/CPU0:Router(config)#
ssh client ?

  v1                Set ssh client to use version 1. This is deprecated and will be removed in
RP/0/RP0/CPU0:Router(config)#
ssh server ?

  v1                         Cisco sshd protocol version 1. This is deprecated in 25.3.1.
```

ssh client v1

ssh server v1

Warning

RP/0/RP0/CPU0:Nov 19 15:20:42.814 UTC: ssh_conf_proxy[1210]: %SECURITY-SSHD_CONF_PRX-4-WARNING_GENERAL : Backup server, netconf-port configs, ssh v1, ssh port are not supported in this platform and release, will not take effect

Yang Model

Cisco-IOS-XR-um-ssh-cfg

Recommendation

Use SSH v2.

Configuration SSHv2: Implementing Secure Shell

TACACS+ and Radius with pre-shared keys (Type 7)

CLI

```
<#root>
RP/0/RP0/CPU0:Router(config)#
tacacs-server host 10.0.0.1

RP/0/RP0/CPU0:Router(config-tacacs-host)#
key ?

  clear      Config deprecated from 7.4.1. Use '0' instead.
  encrypted  Config deprecated from 7.4.1. Use '7' instead.
RP/0/RP0/CPU0:Router(config)#
tacacs-server key ?

  clear      Config deprecated from 7.4.1. Use '0' instead.
  encrypted  Config deprecated from 7.4.1. Use '7' instead.
```

```
tacacs-server key 7 135445410615102B28252B203E270A

tacacs-server host 10.1.1.1 port 49

 key 7 1513090F007B7977

radius-server host 10.0.0.1 auth-port 9999 acct-port 8888

 key 7 1513090F007B7977

aaa server radius dynamic-author

 client 10.10.10.2 vrf default

  server-key 7 05080F1C2243

radius-server key 7 130415110F

aaa group server radius RAD

 server-private 10.2.4.5 auth-port 12344 acct-port 12345
 key 7 1304464058
```

Warning

RP/0/RP0/CPU0:Oct 18 18:00:42.505 UTC: tacacsd[1155]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Feature 'TACACS+ shared secret (Type 7 encoding)' utilized or configured. This feature is known to be insecure, consider ceasing use of this feature. Use Type 6 (AES-based) encryption instead.

RP/0/RP0/CPU0:Oct 18 18:00:42.505 UTC: tacacsd[1155]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Feature 'TACACS+ over TCP with shared secret (default mode)' utilized or configured. This feature is known to be insecure, consider ceasing use of this feature. Use TACACS+ over TLS (Secure TACACS+) for stronger security.

RP/0/RP0/CPU0:Oct 18 18:18:19.460 UTC: radiusd[1149]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Feature 'RADIUS shared secret (Type 7 encoding)' utilized or configured. This feature is known to be insecure, consider ceasing use of this feature. Use Type 6 (AES-based) encryption instead.

RP/0/RP0/CPU0:Oct 18 18:18:19.460 UTC: radiusd[1149]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Feature 'RADIUS over UDP with shared secret (default mode)' utilized or configured. This feature is known to be insecure, consider ceasing use of this feature. Use RADIUS over TLS (RadSec) or DTLS for stronger security.

Yang Model

-

Recommendation

Use TACACS+ or Radius over TLS 1.3 or DTLS. Use Type 6 for credentials.

Configuration TACACS+ or Radius over TLS 1.3 or DTLS: Configuring AAA Services

TLS 1.0/1.1, deprecate weak ciphers

CLI

```
<#root>

RP/0/RP0/CPU0:Router(config)#

http client ssl version ?


  tls1.0  Force TLSv1.0 to be used for HTTPS requests, TLSv1.0 is deprecated from 25.3.1
  tls1.1  Force TLSv1.1 to be used for HTTPS requests, TLSv1.1 is deprecated from 25.3.1

RP/0/RP0/CPU0:Router(config)#

logging tls-server server-name min-version ?


  tls1.0  Set TLSv1.0 to be used as min version for syslog, TLSv1.0 is deprecated from 25.3.1
  tls1.1  Set TLSv1.1 to be used as min version for syslog, TLSv1.1 is deprecated from 25.3.1

RP/0/RP0/CPU0:Router(config)#

logging tls-server server-name max-version ?
```

```
  tls1.0  Set TLSv1.0 to be used as max version for syslog, TLSv1.0 is deprecated from 25.3.1
  tls1.1  Set TLSv1.1 to be used as max version for syslog, TLSv1.1 is deprecated from 25.3.1
```

logging tls-server server-name <> max-version tls1.0|tls1.1

Warning

-

Yang Model

Cisco-IOS-XR-um-logging-cfg

Cisco-IOS-XR-um-http-client-cfg.yang

Recommendation

Use TLS1.2 or TLS1.3.

Configuration Secure Logging: Implementing Secure Logging

Telnet (Server and Client)

CLI

```
<#root>

RP/0/RP0/CPU0:Router(config)#

telnet ?

  ipv4  IPv4 configuration. (Telnet is deprecated since 25.4.1. SSH is recommended instead.)
  ipv6  IPv6 configuration. (Telnet is deprecated since 25.4.1. SSH is recommended instead.)
  vrf   VRF name for telnet server. (Telnet is deprecated since 25.4.1. SSH is recommended inst

RP/0/RP0/CPU0:Router(config)#

telnet ipv4 ?

  client  Telnet client configuration commands. (Telnet is deprecated since 25.4.1. SSH is recon
  server  Telnet server configuration commands. (Telnet is deprecated since 25.4.1. SSH is recon

RP/0/RP0/CPU0:Router(config)#

telnet ipv6 ?

  client  Telnet client configuration commands. (Telnet is deprecated since 25.4.1. SSH is recon
  server  Telnet server configuration commands. (Telnet is deprecated since 25.4.1. SSH is recon

RP/0/RP0/CPU0:Router(config)#

telnet vrf default ?
```

```
  ipv4  IPv4 configuration. (Telnet is deprecated since 25.4.1. SSH is recommended instead.)
  ipv6  IPv6 configuration. (Telnet is deprecated since 25.4.1. SSH is recommended instead.)
```

```
RP/0/RP0/CPU0:Router(config)#

telnet vrf test ?
```

```
  ipv4  IPv4 configuration. (Telnet is deprecated since 25.4.1. SSH is recommended instead.)
  ipv6  IPv6 configuration. (Telnet is deprecated since 25.4.1. SSH is recommended instead.)
```

```
RP/0/RP0/CPU0:Router#

telnet ?
```

```
  A.B.C.D          IPv4 address. (Telnet is deprecated since 25.4.1. SSH is recommended instead
  WORD             Hostname of the remote node. (Telnet is deprecated since 25.4.1. SSH is recon
  X:X::X           IPv6 address. (Telnet is deprecated since 25.4.1. SSH is recommended instead
  disconnect-char  telnet client disconnect char. (Telnet is deprecated since 25.4.1. SSH is rec
  vrf              vrf table for the route lookup. (Telnet is deprecated since 25.4.1. SSH is r
```

telnet

telnet ipv4

telnet ipv6

telnet vrf

Warning

RP/0/RP0/CPU0:Jun 27 10:59:52.226 UTC: cinetd[145]: %IP-CINETD-4-TELNET_WARNING : Telnet support is being deprecated from 25.4.1 onwards. Please use SSH instead.

Yang Model

Cisco-IOS-XR-ipv4-telnet-cfg

Cisco-IOS-XR-ipv4-telnet-mgmt-cfg

Cisco-IOS-XR-um-telnet-cfg

Recommendation

Use SSHv2.

Configuration SSHv2: Implementing Secure Shell

TFTP (Server and Client)

CLI

<#root>

```
RP/0/RP0/CPU0:Router(config)#
ip tftp ?

  client  TFTP client configuration commands (This is deprecated since 25.4.1)
```

tftp

ip tftp

tftp client

Warning

RP/0/RP0/CPU0:Oct 17 19:03:29.475 UTC: tftp_fs[414]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Feature 'TFTP client' utilized or configured. This feature is known to be insecure, consider ceasing use of this feature. Use SFTP instead.

Yang Model

-

Recommendation

Use sFTP or HTTPS.

Configuration sFTP: Implementing Secure Shell

TCP/UDP small servers

CLI

<#root>

```
RP/0/RP0/CPU0:Router(config)#
service ?

  ipv4                   Ipv4 small servers (This is deprecated)
  ipv6                   Ipv6 small servers (This is deprecated)

RP/0/RP0/CPU0:Router(config)#
service ipv4 ?

  tcp-small-servers  Enable small TCP servers (e.g., ECHO)(This is deprecated)
  udp-small-servers  Enable small UDP servers (e.g., ECHO)(This is deprecated)
```

service ipv4

service ipv6

Warning

-

Yang Model

Cisco-IOS-XR-ip-tcp-cfg

Cisco-IOS-XR-ip-udp-cfg

Recommendation

Disable TCP/UDP small servers.

FTP

CLI

<#root>

```
RP/0/RP0/CPU0:Router(config)#
ftp ?

  client  FTP client config commands.This is deprecated since 25.4.1.SFTP is recommended instea
RP/0/RP0/CPU0:Router(config)#
ip ftp ?

  client  FTP client config commands.This is deprecated since 25.4.1.SFTP is recommended instea
```

ip ftp

ftp

Warning

RP/0/RP0/CPU0:Oct 16 21:42:42.897 UTC: ftp_fs[1190]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Feature 'FTP client' utilized or configured. This feature is known to be insecure, consider ceasing use of this feature. Use SFTP instead.

Yang Model

Cisco-IOS-XR-um-ftp-tftp-cfg

Recommendation

Use sFTP or HTTPS.

Configuration sFTP: Implementing Secure Shell

SNMP v1/2c

CLI

```
<#root>

RP/0/RP0/CPU0:Router(config)#

snmp-server ?


  chassis-id              String to uniquely identify this chassis
  community               Enable SNMP;  set community string and access privileges. (This is depre

RP/0/RP0/CPU0:Router(config)#

snmp-server ?


  community               Enable SNMP;  set community string and access privileges. (This is depre

RP/0/RP0/CPU0:Router(config)#

snmp-server user test test ?


  v1      user using the v1 security model (This is deprecated since 25.4.1)
  v2c     user using the v2c security model (This is deprecated since 25.4.1)
  v3      user using the v3 security model

RP/0/RP0/CPU0:Router(config)#

snmp-server host 10.0.0.1 version ?


  1   Use 1 for SNMPv1. (This is deprecated since 25.4.1)
  2c  Use 2c for SNMPv2c. (This is deprecated since 25.4.1)
  3   Use 3 for SNMPv3

RP/0/RP0/CPU0:Router(config)#

snmp-server group test ?


  v1   group using the v1 security model (This is deprecated since 25.4.1)
  v2c  group using the v2c security model (This is deprecated since 25.4.1)
  v3   group using the User Security Model (SNMPv3)

RP/0/RP0/CPU0:Router(config)#

snmp-server ?


  community               Enable SNMP;  set community string and access privileges. (This is depre
  community-map           Community Mapping as per RFC-2576. (This is deprecated since 25.4.1)

RP/0/RP0/CPU0:Router(config)#

snmp-server user user1 group1 ?


  v1      user using the v1 security model (This is deprecated since 25.4.1)
  v2c     user using the v2c security model (This is deprecated since 25.4.1)
```

```
RP/0/RP0/CPU0:Router(config)#

snmp-server user user1 group1 v3 auth md5 test priv ?


  3des    Use 168 bit 3DES algorithm for encryption (This is deprecated since 25.4.1)
  des56   Use 56 bit DES algorithm for encryption (This is deprecated since 25.4.1)

RP/0/RP0/CPU0:Router(config)#

snmp ?


  community             Enable SNMP;  set community string and access privileges. (This is depre

RP/0/RP0/CPU0:Router(config)#

snmp user user test ?


  remote  Specify a remote SNMP entity to which the user belongs
  v1      user using the v1 security model (This is deprecated since 25.4.1)
  v2c     user using the v2c security model (This is deprecated since 25.4.1)

RP/0/RP0/CPU0:Router(config)#

snmp-server user user1 group1 v3 auth ?


  md5      Use HMAC MD5 algorithm for authentication (This is deprecated since 25.4.1)
  sha      Use HMAC SHA algorithm for authentication (This is deprecated since 25.4.1)

RP/0/RP0/CPU0:Router(config)#

snmp user user1 group1 v3 auth ?


  md5      Use HMAC MD5 algorithm for authentication (This is deprecated since 25.4.1)
  sha      Use HMAC SHA algorithm for authentication (This is deprecated since 25.4.1)

RP/0/RP0/CPU0:Router(config)#

snmp user user1 group1 v3 auth md5 test priv ?


  3des    Use 168 bit 3DES algorithm for encryption (This is deprecated since 25.4.1)
  des56   Use 56 bit DES algorithm for encryption (This is deprecated since 25.4.1)

RP/0/RP0/CPU0:Router(config)#

snmp host 10.1.1.1 version ?


  1   Use 1 for SNMPv1. (This is deprecated since 25.4.1)
  2c  Use 2c for SNMPv2c. (This is deprecated since 25.4.1)

RP/0/RP0/CPU0:Router(config)#

snmp-server host 10.1.1.1 version ?


  1   Use 1 for SNMPv1. (This is deprecated since 25.4.1)
  2c  Use 2c for SNMPv2c. (This is deprecated since 25.4.1)

RP/0/RP0/CPU0:Router(config)#
```

```
snmp ?

  community-map          Community Mapping as per RFC-2576. (This is deprecated since 25.4.1)
```

snmp-server community

snmp-server user <> <> v1 | v2c

snmp-server user <> <> v3 auth md5 | sha

snmp-server user <> <> v3 auth md5|sha <> priv 3des|des56

snmp-server host <> version 1|v2c

snmp-server group <> v1|v2c

snmp-server community-map

snmp community

snmp user <> <> v1|v2c

snmp user <> <> v3 auth md5|sha

snmp user <> <> v3 auth md5/sha <> priv 3des|des56

snmp host <> version 1|v2c

snmp group <> v1|v2c

snmp community-map

Warning

-

Yang Model

Cisco-IOS-XR-um-snmp-server-cfg

Recommendation

Use SNMPv3 with authentication and encryption (authPriv).

Configuration SNMPv3 with authentication and authPriv: Configuring Simple Network Management Protocol

NTP Version 2 and 3 and MD5 Authentication

CLI

<#root>

```
RP/0/RP0/CPU0:Router(config)#
ntp server 10.1.1.1 version ?

  <2-4>  NTP version number. Values 2-3 are DEPRECATED from 25.4.1 onwards; use 4 instead.
RP/0/RP0/CPU0:Router(config)#
ntp peer 10.1.1.1 version ?

  <2-4>  NTP version number. Values 2-3 are DEPRECATED from 25.4.1 onwards; use 4 instead.
RP/0/RP0/CPU0:Router(config)#
ntp server admin-plane version ?

  <1-4>  NTP version number. Values 1-3 are DEPRECATED from 25.4.1 onwards; use 4 instead.
RP/0/RP0/CPU0:Router(config)#
ntp interface gigabitEthernet 0/0/0/0 broadcast version ?

  <2-4>  NTP version number. Values 2-3 are DEPRECATED from 25.4.1 onwards; use 4 instead.
RP/0/RP0/CPU0:Router(config)#
ntp interface gigabitEthernet 0/0/0/0 multicast version ?

  <2-4>  NTP version number. Values 2-3 are DEPRECATED from 25.4.1 onwards; use 4 instead.
RP/0/RP0/CPU0:Router(config)#
ntp authentication-key 1 md5 clear 1234
```

ntp server <> version 2|3

ntp peer <> version 2/3

ntp server admin-plane version 1/2/3

ntp interface <> broadcast version 2|3

ntp interface <> multicast version 2|3

ntp authentication-key <> md5 <> <>

Warning

```
RP/0/RP0/CPU0:Nov 25 16:09:15.422 UTC: ntpd[159]: %IP-IP_NTP-5-CONFIG_NOT_RECOMMENDED : NTPv2 and NTPv3 are deprecated from 25.4.1 onwards. Please use NTPv4.

RP/0/RP0/CPU0:Nov 25 16:09:15.422 UTC: ntpd[159]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Feature 'NTP with no authentication' utilized or configured. This feature is known to be insecure, consider ceasing use of this feature.
```

Yang Model

Cisco-IOS-XR-um-ntp-cfg.yang

Recommendation

Use NTP version 4 or an authentication other than MD5.

Configuration NTP: [Configuring Network Time Protocol]

GRPC

CLI

<#root>

```
RP/0/RP0/CPU0:Router(config)#
```

`grpc ?`

```
  aaa                           AAA authorization and authentication for gRPC
  address-family                DEPRECATED. Removing in 26.3.1: Address family identifier type
  apply-group                   Apply configuration from a group
  certificate                   DEPRECATED. Removing in 26.3.1: gRPC server certificate
  certificate-authentication    DEPRECATED. Removing in 26.3.1: Enables Certificate based Authentication
  certificate-id                DEPRECATED. Removing in 26.3.1: Active Certificate
  default-server-disable        Configuration to disable the default gRPC server
  dscp                          DEPRECATED. Removing in 26.3.1: QoS marking DSCP to be set on transmitted
  exclude-group                 Exclude apply-group configuration from a group
  gnmi                          gNMI service configuration
  gnpsi                         gnpsi configuration
  gnsi                          gNSI
  gribi                         gRIBI service configuration
  keepalive                     DEPRECATED. Removing in 26.3.1: Server keepalive time and timeout
  listen-addresses              DEPRECATED. Removing in 26.3.1: gRPC server listening addresses
  local-connection              DEPRECATED. Removing in 26.3.1: Enable gRPC server over Unix socket
  max-concurrent-streams        gRPC server maximum concurrent streams per connection
  max-request-per-user          Maximum concurrent requests per user
  max-request-total             Maximum concurrent requests in total
  max-streams                   Maximum number of streaming gRPCs (Default: 32)
  max-streams-per-user          Maximum number of streaming gRPCs per user (Default: 32)
  memory                        EMSd-Go soft memory limit in MB
  min-keepalive-interval        DEPRECATED. Removing in 26.3.1: Minimum client keepalive interval
  name                          DEPRECATED. Removing in 26.3.1: gRPC server name
  no-tls                        DEPRECATED. Removing in 26.3.1: No TLS
  p4rt                          p4 runtime configuration
  port                          DEPRECATED. Removing in 26.3.1: Server listening port
  remote-connection             DEPRECATED. Removing in 26.3.1: Configuration to toggle TCP support on th
  segment-routing               gRPC segment-routing configuration
  server                        gRPC server configuration
  service-layer                 grpc service layer configuration
  tls-cipher                    DEPRECATED. Removing in 26.3.1: gRPC TLS 1.0-1.2 cipher suites
  tls-max-version               DEPRECATED. Removing in 26.3.1: gRPC maximum TLS version
  tls-min-version               DEPRECATED. Removing in 26.3.1: gRPC minimum TLS version
  tls-mutual                    DEPRECATED. Removing in 26.3.1: Mutual Authentication
  tls-trustpoint                DEPRECATED. Removing in 26.3.1: Configure trustpoint
  tlsV1-disable                 Disable support for TLS version 1.0
```

```
                              tlsv1-disable CLI is deprecated.
                              Use tls-min-version CLI to set minimum TLS version.
  ttl                         DEPRECATED. Removing in 26.3.1: gRPC packets TTL value
  tunnel                      DEPRECATED. Removing in 26.3.1: grpc tunnel service
  vrf                         DEPRECATED. Removing in 26.3.1: Server vrf
  <cr>
```

grpc no-tls
grpc tls-max|min-version 1.0|1.1
grpc tls-cihper default|enable|disable (In TLS 1.2, insecure when unsafe cipher suites are used after evaluating the three configs)

Warning

RP/0/RP0/CPU0:Nov 29 19:38:30.833 UTC: emsd[1122]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Feature 'gRPC insecure configuration' utilized or configured. This feature is deprecated as it is known to be insecure; it will be removed in a future release. server=DEFAULT (TLS version is older than 1.2, unsafe cipher suites are configured)

Yang Model

Cisco-IOS-XR-um-grpc-cfg.yang

Cisco-IOS-XR-man-ems-oper.yang

Cisco-IOS-XR-man-ems-grpc-tls-credentials-rotate-act.yang

Cisco-IOS-XR-man-ems-cfg.yang

Recommendation

Use TLS 1.2 or higher (preferably TLS 1.3) with strong ciphers.

Configuration: Use gRPC Protocol to Define Network Operations with Data Models

List of Insecure Execute Commands

Copy Commands

CLI

<#root>

`RP/0/RP0/CPU0:Router#`

`copy ?`

```
  ftp:            Copy from ftp: file system (Deprecated since 25.4.1)
  tftp:           Copy from tftp: file system (Deprecated since 25.4.1)
```

<#root>

```
RP/0/RP0/CPU0:Router#

copy running-config ?


  ftp:       Copy to ftp: file system (Deprecated since 25.4.1)
  tftp:      Copy to tftp: file system (Deprecated since 25.4.1)
```

copy <src as tftp/ftp> <dst as tftp/ftp>
copy running-config <tftp/ftp>

copy <tftp/ftp> running-config

Warning

RP/0/RP0/CPU0:Nov 26 15:05:57.666 UTC: filesys_cli[66940]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Feature 'copy ftp' utilized or configured. This feature is deprecated as it is known to be insecure; it will be removed in a future release. Use SFTP or SCP instead.

RP/0/RP0/CPU0:Nov 26 15:09:06.181 UTC: filesys_cli[67445]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Feature 'copy tftp' utilized or configured. This feature is deprecated as it is known to be insecure; it will be removed in a future release. Use SFTP or SCP instead.

Yang Model

-

Recommendation

Use sFTP or SCP.

Configuration: Implementing Secure Shell

Install Commands

CLI

```
install source <tftp/ftp>
install add source <tftp/ftp>
install replace <tftp/ftp>"
```

Warning

-

Yang Model

Cisco-IOS-XR-sysadmin-instmgr-oper.yang

Recommendation

Use sFTP or SCP.

Configuration: Implementing Secure Shell

Load Commands

CLI

<#root>

```
RP/0/RP0/CPU0:Router#

configure


RP/0/RP0/CPU0:Router(config)#
RP/0/RP0/CPU0:Router(config)#

load ?


  ftp:           Load from ftp: file system (Deprecated since 25.4.1)
  tftp:          Load from tftp: file system (Deprecated since 25.4.1)
```

<#root>

```
RP/0/RP0/CPU0:ROUTER(config)#

load script ?


  ftp:       Load from ftp: file system (Deprecated since 25.4.1)
  tftp:      Load from tftp: file system (Deprecated since 25.4.1)
```

<#root>

```
RP/0/RP0/CPU0:ROUTER(config)#

load diff ?


  ftp:       Load from ftp: file system (Deprecated since 25.4.1)
  tftp:      Load from tftp: file system (Deprecated since 25.4.1)
```

<#root>

```
RP/0/RP0/CPU0:Router(config)#

load diff reverse ?


  ftp:       Load from ftp: file system (Deprecated since 25.4.1)
  tftp:      Load from tftp: file system (Deprecated since 25.4.1)
```

```
load <ftp/tftp>

load script <ftp/tftp>

load diff <ftp/tftp>

load diff reverse <ftp/tftp>
```

Warning

```
RP/0/RP0/CPU0:Dec 18 10:58:45.938 UTC: config[68291]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Feature 'load ftp:' utilized or configured. This feature is deprecated as it is known to be insecure; it will be removed in a future release. Loading over ftp: is insecure and deprecated. Use scp or sftp instead.

RP/0/RP0/CPU0:Dec 18 10:58:51.584 UTC: config[68291]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Feature 'load tftp:' utilized or configured. This feature is deprecated as it is known to be insecure; it will be removed in a future release. Loading over tftp: is insecure and deprecated. Use scp or sftp instead.

RP/0/RP0/CPU0:Dec 18 10:52:11.086 UTC: config[67526]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Feature 'load script ftp:' utilized or configured. This feature is deprecated as it is known to be insecure; it will be removed in a future release. Loading scripts over ftp: is insecure and deprecated. Use scp or sftp instead.

RP/0/RP0/CPU0:Dec 18 10:53:38.825 UTC: config[68291]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Feature 'load script tftp:' utilized or configured. This feature is deprecated as it is known to be insecure; it will be removed in a future release. Loading scripts over tftp: is insecure and deprecated. Use scp or sftp instead.

RP/0/RP0/CPU0:Dec 18 08:24:37.414 UTC: config[65969]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Feature 'load diff ftp:' utilized or configured. This feature is deprecated as it is known to be insecure; it will be removed in a future release. Loading diff over ftp: is insecure and deprecated. Use scp or sftp instead.

RP/0/RP0/CPU0:Dec 18 10:55:37.248 UTC: config[68291]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Feature 'load diff tftp:' utilized or configured. This feature is deprecated as it is known to be insecure; it will be removed in a future release. Loading diff over tftp: is insecure and deprecated. Use scp or sftp instead.

RP/0/RP0/CPU0:Dec 18 10:56:21.806 UTC: config[68291]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Feature 'load diff reverse ftp:' utilized or configured. This feature is deprecated as it is known to be insecure; it will be removed in a future release. Loading diff over ftp: is insecure and deprecated. Use scp or sftp instead.

RP/0/RP0/CPU0:Dec 18 10:56:12.031 UTC: config[68291]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Feature 'load diff reverse tftp:' utilized or configured. This feature is deprecated as it is known to be insecure; it will be removed in a future release. Loading diff over tftp: is insecure and deprecated. Use scp or sftp instead.
```

Yang Model

-

Recommendation

Use sFTP or SCP.

Configuration: Implementing Secure Shell

Utility Commands

CLI

```
utility mv source <tftp/ftp>
utility mv source <interactive|force> source <tftp/ftp>
```

Warning

RP/0/RP0/CPU0:Dec 18 10:30:22.499 UTC: run_utility[68509]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Feature 'utility mv tftp' utilized or configured. This feature is deprecated as it is known to be insecure; it will be removed in a future release.

RP/0/RP0/CPU0:Dec 18 10:30:35.803 UTC: run_utility[68549]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Feature 'utility mv ftp' utilized or configured. This feature is deprecated as it is known to be insecure; it will be removed in a future release.

Yang Model

-

Recommendation

Use sFTP or SCP.

Configuration: Implementing Secure Shell

Yang Models

There are too many changes in the Yang models to list them all here.

This is an example for the comments in the Yang model*Cisco-IOS-XR-ipv4-ma-cfg.yang*for the removal of source routing.

```
revision "2025-09-01" {
    description
      "Deprecated IPv4 Source Route Configuration.

leaf source-route {
      type boolean;
      default "true";
      status deprecated;
      description
        "The flag for enabling whether to process packets
        with source routing header options (This is
        deprecated since 25.4.1)";
```

This is an example for the comments in the Yang model*Cisco-IOS-XR-um-ftp-tftp-cfg*.yang for the removal of FTP and TFTP.

```
revision 2025-08-29 {
    description
      "TFTP config commands are deprecated.
       2025-08-20
         FTP config commands are deprecated.";

container ftp {
    status deprecated;
    description
      "Global FTP configuration commands.This is deprecated since 25.4.1.
       SFTP is recommended instead.";
    container client {
      status deprecated;
      description
        "FTP client configuration commands.This is deprecated since 25.4.1.
         SFTP is recommended instead.";

       container ipv4 {
          status "deprecated";
          description
            "Ipv4 (This is deprecated since 25.4.1)";

container ipv6 {
          status "deprecated";
          description
            "Ipv6  (This is deprecated since 25.4.1)";

container tftp-fs {
    status deprecated;
    description
      "Global TFTP configuration commands (This is deprecated since 25.4.1)";
    container client {
      status deprecated;
      description
        "TFTP client configuration commands (This is deprecated since 25.4.1)";
      container vrfs {
        status "deprecated";
        description
          "VRF name for TFTP service (This is deprecated since 25.4.1)";
```

IOS XR Hardening Guide

The guide Cisco IOS XR Software Hardening Guide helps network administrators and security practitioners secure Cisco IOS XR-based routers to increase the overall security posture of the network.

This document is structured around the three planes by which the functions of a network device are categorized.

The three functional planes of a router are the management plane, control plane, and data plane. Each provides a different functionality that must be protected.

- **Management Plane:** The management plane contains the logical group of all traffic that supports provisioning, maintenance, and monitoring functions for the Cisco IOS XR device and the network. Traffic in this group includes Secure Shell (SSH), Secure Copy Protocol (SCP), Simple Network Management Protocol (SNMP), Syslog, TACACS+, RADIUS, DNS, NetFlow, and Cisco Discovery Protocol. Management plane traffic is always destined to the local Cisco IOS XR device.
- **Control Plane:** The control plane contains the logical group of all routing, signaling, link-state, and other control protocols that are used to create and maintain the state of the network and its interfaces. These include Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), Label Distribution Protocol (LDP), Intermediate System to Intermediate System (IS-IS), Network Time Protocol (NTP), Address Resolution Protocol (ARP), and Layer 2 keepalives. Control plane traffic is always destined to the local Cisco IOS XR device.
- **Data Plane:** The data plane contains the logical group of "customer" application traffic generated by hosts, clients, servers, and applications that are sourced from and destined to other similar devices supported by the network. Data plane features include IP source routing, IP directed broadcast, ICMP redirects, ICMP unreachables, and proxy ARP. Data plane traffic is mainly forwarded in the fast path and is never destined to the local Cisco IOS XR device.

Config Resilient Infrastructure Tester

You can test the router configuration in order to see if it is secure or not with this tool which works for several operating systems, including IOS XR: Cisco Config Resilient Infrastructure Tester.

Question and Answer

1. If you configure a command the second time or you configure the same command again, does it trigger the same syslog warning message again?

A: No.

2. Will two configuration commands for two different features in the same commit cause two syslog warnings?

A: Yes.

Example:

```
RP/0/RP0/CPU0:Oct 17 19:01:48.806 UTC: ipv6_io[310]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Feature 'IPV6 SOURCE ROUTE' utilized or configured. This feature is known to be insecure, consider ceasing use of this feature. Do not enable IPv6 Source Routing due to security risks.
```

```
RP/0/RP0/CPU0:Oct 17 19:01:48.806 UTC: ipv4_ma[254]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Feature 'IPV4 SOURCE ROUTE' utilized or configured. This feature is known to be insecure, consider ceasing use of this feature. Do not enable IPv4 Source Routing due to security risks.
```

3. Will a new insecure configuration command in a new commit cause a new warning?

A: Yes.

4. Is there a syslog warning when the insecure feature is removed from the configuration?

A: Yes

Examples:

```
RP/0/RP0/CPU0:Oct 18 08:16:24.410 UTC: ssh_conf_proxy[1210]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED : Insecure feature 'SSH host-key DSA algorithm' configuration removed.
```

```
RP/0/RP0/CPU0:Oct 22 06:37:21.960 UTC: tacacsd[1155]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED : Insecure feature 'TACACS+ shared secret (Type 7 encoding)' configuration removed.
```

```
RP/0/RP0/CPU0:Oct 22 06:42:21.805 UTC: tacacsd[1155]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED : Insecure feature 'TACACS+ over TCP with shared secret (default mode)' configuration removed.
```

5. You do not see Telnet available on your router.

A: It is possible that you run IOS XR XR7/LNT which has Telnet only available if you loaded the optional Telnet RPM.

6. You do not see XR7/LNT having the sFTP or SCP option for the command “install source”.

A: At this moment XR7/LNT does not support sFTP or SCP for the “install source” command.

7. Do the changes apply equally to IOS XR eXR and IOS XR XR7/LNT?

A: Yes.

8. How can you check if your router runs IOS XR eXR or IOS XR XR7/LNT

A: Use “show version” and look for “LNT”. 8000 routers and some NCS540 variants run IOS XR XR7/LNT.

Example:

<#root>

```
RP/0/RP0/CPU0:Router#

show version


Cisco IOS XR Software, Version 25.2.2

LNT
```