Resistencia de la infraestructura Cisco IOS XR

Contenido

Introducción

Este documento describe un aspecto de endurecimiento de Cisco IOS® XR: eliminar sistemáticamente las características y los cifrados inseguros.

Resistencia de la infraestructura Cisco IOS XR

Para aumentar la condición en materia de seguridad de los dispositivos de Cisco, Cisco está realizando cambios en la configuración predeterminada, desaprobando y, finalmente, eliminando las funciones no seguras e introduciendo nuevas funciones de seguridad. Estos cambios están diseñados para reforzar la infraestructura de la red y ofrecer una mejor visibilidad de las actividades de los agentes de amenazas.

Consulte esta página del centro de confianza: Infraestructura resistente. Menciona el

endurecimiento de la infraestructura, la Guía de endurecimiento del software Cisco IOS XR, el proceso de desaprobación de funciones y los detalles de eliminación y desaprobación de funciones. Aquí se mencionan las alternativas sugeridas: Eliminación de funciones y Alternativas sugeridas.

Cisco IOS XR está eliminando progresivamente las características y los cifrados inseguros. Esto incluye los comandos configuration y execute en Cisco IOS XR.

Funciones afectadas

- TELNET
- TFTP
- FTP
- HTTP
- SNMP v1/v2c
- SNMP v3 sin authPriv
- Ruta de origen IP
- Pequeños servidores TCP/UDP
- TACACS+ y Radius con claves previamente compartidas (tipo 7) y MD5
- SSH v1
- TLS 1.0/1.1
- NTPv2/3 y MD5
- GRPC sin TLS, TLSv1.0/1.1
- Comandos Exec que utilizan copy, utility e install con TFTP/FTP

Agrupación

Existen comandos de configuración, pero también comandos de ejecución (por ejemplo, el comando "copy").

Los comandos desaprobados se pueden agrupar:

- SSHv1, Telnet (servidor y cliente), TFTP (cliente), FTP
- DSA host-key, TACACS/RADIUS tipo 7, TLS 1.0/1.1
- Otro: Pequeños servidores TCP/UDP, routing de origen IP (IPv4 e IPv6)

Fases

Este proyecto sigue el enfoque habitual de deprecación de funciones: warn -> restrict -> remove.

- Advertencias en Cisco IOS XR versión 25.4.1.
- Fase de restricción
- Eliminación de funciones

Fase de advertencia

¿Cuáles son las advertencias?

1. Función de ayuda de CLI (interfaz de línea de comandos)

2. Una advertencia de syslog
3. Una advertencia de descripción en el módulo yang

Se emiten advertencias para las opciones no seguras configuradas. Estos son mensajes de syslog con **una frecuencia de 30 días**.

Cuando se utiliza cualquier función no segura, se emite esta advertencia de registro (nivel 4 o advertencia):

*%**INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN**: Característica '<feature-name>' utilizada o configurada. Se sabe que esta función no es segura. Considere la posibilidad de dejar de usarla. <Recomendación>*

La recomendación es qué utilizar en lugar de la opción insegura.

Ejemplo de advertencia para FTP:

%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Función 'FTP' utilizada o configurada. Se sabe que esta función no es segura. Considere la posibilidad de dejar de usarla. Se recomienda utilizar SFTP.

Observe las palabras utilizadas o configuradas. Utilizado se refiere a un comando de ejecución y configurado se refiere a un comando de configuración.

Se puede imprimir un mensaje de advertencia si se elimina la opción insegura (nivel 6 o informativo). Ejemplo:

RP/0/RP0/CPU0:22 de octubre 06:43:43.967 UTC: tacacsd[1155]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED: Se ha eliminado la configuración de la función 'TACACS+ sobre TCP con secreto compartido (modo predeterminado)'.

Lista de opciones no seguras desaprobadas

Esta es la lista de opciones inseguras que activan una advertencia en las versiones de Cisco IOS XR de la fase de advertencia.

La lista muestra la opción insegura, los comandos configuration o execute, el mensaje de advertencia y el modelo Yang asociado.

Routing de origen IP (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

Advertencia

RP/0/RP0/CPU0:17 de octubre 19:01:48.806 UTC: ipv4_ma[254]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Función 'IPV4 SOURCE ROUTE' utilizada o configurada. Se sabe que esta función no es segura. Considere la posibilidad de dejar de usarla. No habilite el routing de origen IPv4 debido a riesgos de seguridad.

RP/0/RP0/CPU0:17 de octubre 19:01:48.806 UTC: ipv6_io[310]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Característica 'IPV6 SOURCE ROUTE' utilizada o configurada. Se sabe que esta función no es segura. Considere la posibilidad de dejar de usarla. No habilite el routing de origen IPv6 debido a riesgos de seguridad.

Modelo Yang

Cisco-IOS-XR-ipv4-ma-cfg

Cisco-IOS-XR-ipv6-io-cfg

Cisco-IOS-XR-um-ipv4-cfg

Cisco-IOS-XR-um-ipv6-cfg

Recomendación

Elimine la opción no segura.

No existe una alternativa exacta. Los clientes que deseen controlar el tráfico a través de una red basada en la dirección de origen pueden hacerlo mediante el routing basado en políticas u otros mecanismos de routing de origen controlados por el administrador que no dejan la decisión de routing al usuario final.

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

Advertencia

RP/0/RP0/CPU0:19 de noviembre 15:20:42.814 UTC: ssh_conf_proxy[1210]: %SECURITY-SSHD_CONF_PRX-4-WARNING_GENERAL: El servidor de respaldo, las configuraciones netconf-port, ssh v1, el puerto ssh no son soportados en esta plataforma y la versión, no tendrá efecto

Modelo Yang

Cisco-IOS-XR-um-ssh-cfg

Recomendación

Utilice SSH v2.

Configuración SSHv2: Implementación de Secure Shell

TACACS+ y Radius con claves previamente compartidas (tipo 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

clave 7 1513090F007B7977

radius-server host 10.0.0.1 auth-port 999 acct-port 8888

clave 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

Advertencia

RP/0/RP0/CPU0:18 de octubre 18:00:42.505 UTC: tacacsd[1155]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Característica 'secreto compartido TACACS+ (codificación Tipo 7)' utilizada o configurada. Se sabe que esta función no es segura. Considere la posibilidad de dejar de usarla. En su lugar, utilice el cifrado de tipo 6 (basado en AES).

RP/0/RP0/CPU0:18 de octubre 18:00:42.505 UTC: tacacsd[1155]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Característica 'TACACS+ sobre TCP con secreto compartido (modo predeterminado)' utilizada o configurada. Se sabe que esta función no es segura. Considere la posibilidad de dejar de usarla. Utilice TACACS+ sobre TLS (TACACS+ seguro) para una mayor seguridad.

RP/0/RP0/CPU0:18 de octubre 18:18:19.460 UTC: RADIUS[1149]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Característica 'Secreto compartido RADIUS (codificación Tipo 7)' utilizada o configurada. Se sabe que esta función no es segura. Considere la posibilidad de dejar de usarla. En su lugar, utilice el cifrado de tipo 6 (basado en AES).

RP/0/RP0/CPU0:18 de octubre 18:18:19.460 UTC: RADIUS[1149]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Característica 'RADIUS sobre UDP con secreto compartido (modo predeterminado)' utilizada o configurada. Se sabe que esta función no es segura. Considere la posibilidad de dejar de usarla. Utilice RADIUS sobre TLS (RadSec) o DTLS para una mayor seguridad.

Modelo Yang

-

Recomendación

Utilice TACACS+ o Radius sobre TLS 1.3 o DTLS. Utilice el tipo 6 para las credenciales.

Configuración de TACACS+ o Radius sobre TLS 1.3 o DTLS: Configuración de Servicios AAA

TLS 1.0/1.1, invalida los cifrados débiles

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

Advertencia

-

Modelo Yang

Cisco-IOS-XR-um-logging-cfg

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

Recomendación

Utilice TLS1.2 o TLS1.3.

Configuración de registro seguro: Implementación de registro seguro

Telnet (servidor y cliente)

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 reco
  server  Telnet server configuration commands. (Telnet is deprecated since 25.4.1. SSH is reco

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

telnet ipv6 ?

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

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 reco
  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 re
  vrf              vrf table for the route lookup. (Telnet is deprecated since 25.4.1. SSH is r
```

telnet

Telnet IPv4

Telnet IPv6

telnet vrf

Advertencia

RP/0/RP0/CPU0:27 de junio 10:59:52.226 UTC: cinetd[145]: %IP-CINETD-4-TELNET_WARNING: El soporte de Telnet está siendo desaprobado desde la versión 25.4.1 en adelante. Utilice SSH en su lugar.

Modelo Yang

Cisco-IOS-XR-ipv4-telnet-cfg

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

Cisco-IOS-XR-um-telnet-cfg

Recomendación

Utilice SSHv2.

Configuración SSHv2: Implementación de Secure Shell

TFTP (servidor y cliente)

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

cliente TFTP

Advertencia

RP/0/RP0/CPU0:17 de octubre 19:03:29.475 UTC: tftp_fs[414]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Característica 'cliente TFTP' utilizada o configurada. Se sabe que esta función no es segura. Considere la posibilidad de dejar de usarla. Utilice SFTP en su lugar.

Modelo Yang

-

Recomendación

Utilice sFTP o HTTPS.

Configuración sFTP: Implementación de Secure Shell

Pequeños servidores TCP/UDP

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

Advertencia

-

Modelo Yang

Cisco-IOS-XR-ip-tcp-cfg

Cisco-IOS-XR-ip-udp-cfg

Recomendación

Desactive los servidores pequeños TCP/UDP.

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

Advertencia

RP/0/RP0/CPU0:16 de octubre 21:42:42.897 UTC: ftp_fs[190]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Característica 'cliente FTP' utilizada o configurada. Se sabe que esta función no es segura. Considere la posibilidad de dejar de usarla. Utilice SFTP en su lugar.

Modelo Yang

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

Recomendación

Utilice sFTP o HTTPS.

Configuración sFTP: Implementación de 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 depr
```

```
RP/0/RP0/CPU0:Router(config)#
snmp-server ?

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

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 depr
  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 depr

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

comunidad SNMP

snmp user <> <> v1|v2c

snmp user <> <> v3 auth md5|sha

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

snmp host <> versión 1|v2c

snmp group <> v1|v2c

snmp community-map

Advertencia

-

Modelo Yang

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

Recomendación

Utilice SNMPv3 con autenticación y cifrado (authPriv).

Configuración de SNMPv3 con autenticación y authPriv: Configuración de Simple Network Management Protocol

Autenticación MD5 y NTP versión 2 y 3

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 **<>** versión 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 **<>** **<>**

Advertencia

RP/0/RP0/CPU0:25 de noviembre 16:09:15.42 UTC: ntpd[159]: %IP-IP_NTP-5-CONFIG_NOT_RECOMMENDED: NTPv2 y NTPv3 están obsoletos a partir de la versión 25.4.1. Utilice NTPv4.

RP/0/RP0/CPU0:25 de noviembre 16:09:15.42 UTC: ntpd[159]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Característica 'NTP sin autenticación' utilizada o configurada. Se sabe que esta función no es segura. Considere la posibilidad de dejar de usarla.

Modelo Yang

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

Recomendación

Utilice NTP versión 4 o una autenticación que no sea MD5.

Configuración NTP: Configuración del Protocolo de Tiempo de Red

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-cipher default|enable|disable (En TLS 1.2, insecure cuando se utilizan conjuntos de cifrado no seguros después de evaluar las tres configuraciones)

Advertencia

RP/0/RP0/CPU0:29 de noviembre 19:38:30.833 UTC: emsd[121]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Característica 'gRPC insecure configuration' utilizada o configurada. Esta característica está obsoleta porque se sabe que es insegura; se eliminará en una futura versión. server=DEFAULT (la versión de TLS es anterior a la 1.2, se configuran conjuntos de cifrado no seguros)

Modelo Yang

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

Recomendación

Utilice TLS 1.2 o superior (preferiblemente TLS 1.3) con cifrados seguros.

Configuración: Uso del Protocolo gRPC para definir operaciones de red con modelos de datos

Lista de comandos de ejecución inseguros

Copiar comandos

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)
```

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

Advertencia

RP/0/RP0/CPU0:26 de noviembre 15:05:57.66 UTC: filesys_cli[66940]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Función 'copy ftp' utilizada o configurada. Esta característica está obsoleta porque se sabe que es insegura; se eliminará en una futura versión. Utilice SFTP o SCP en su lugar.

RP/0/RP0/CPU0:26 de noviembre 15:09:06.181 UTC: filesys_cli[67445]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Característica 'copy tftp' utilizada o configurada. Esta característica está obsoleta porque se sabe que es insegura; se eliminará en una futura versión. Utilice SFTP o SCP en su lugar.

Modelo Yang

-

Recomendación

Utilice sFTP o SCP.

Configuración: Implementación de Secure Shell

Comandos de instalación

CLI

```
install source

install add source

install replace

       "
```

Advertencia

-

Modelo Yang

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

Recomendación

Utilice sFTP o SCP.

Configuración: Implementación de Secure Shell

Comandos de utilidad

CLI

```
utility mv source
```

Modelos Yang

Hay demasiados cambios en los modelos Yang para enumerarlos todos aquí.

Este es un ejemplo para los comentarios en el *modelo* Yang*Cisco-IOS-XR-ipv4-ma-cfg*.yang para la eliminación del ruteo de origen.

```
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)";
```

Este es un ejemplo para los comentarios en el *modelo* Yang *Cisco-IOS-XR-um-ftp-tftp-cfg*.yang para la eliminación de FTP y 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)";
```

Guía de endurecimiento de IOS XR

La guía Cisco IOS XR Software Hardening Guide ayuda a los administradores de red y a los profesionales de la seguridad a proteger los routers basados en Cisco IOS XR para aumentar la condición general de seguridad de la red.

Este documento se estructura en torno a los tres planos por los que se categorizan las funciones de un dispositivo de red.

Los tres planos funcionales de un router son el plano de administración, el plano de control y el plano de datos. Cada una proporciona una funcionalidad diferente que debe protegerse.

- **Plano de administración:** el plano de administración contiene el grupo lógico de todo el tráfico que admite las funciones de aprovisionamiento, mantenimiento y supervisión para el dispositivo Cisco IOS XR y la red. El tráfico de este grupo incluye Secure Shell (SSH), Secure Copy Protocol (SCP), Simple Network Management Protocol (SNMP), Syslog, TACACS+, RADIUS, DNS, NetFlow y Cisco Discovery Protocol. El tráfico del plano de administración siempre está destinado al dispositivo Cisco IOS XR local.
- **Plano de control:** El plano de control contiene el grupo lógico de todos los protocolos de routing, señalización, estado de link y otros protocolos de control que se utilizan para crear y mantener el estado de la red y sus interfaces. Entre ellos se incluyen el protocolo de gateway fronterizo (BGP), ruta de acceso más corta primero (OSPF), protocolo de distribución de etiquetas (LDP), sistema intermedio a sistema intermedio (IS-IS), protocolo de tiempo de la red (NTP), protocolo de resolución de direcciones (ARP) y señales de mantenimiento de capa 2. El tráfico del plano de control siempre está destinado al dispositivo Cisco IOS XR local.
- **Plano de datos:** El plano de datos contiene el grupo lógico de tráfico de aplicaciones "cliente" generado por hosts, clientes, servidores y aplicaciones que se originan y se destinan a otros dispositivos similares admitidos por la red. Las funciones del plano de datos incluyen routing de origen IP, difusión dirigida IP, redirecciones ICMP, ICMP de destino inalcanzable y ARP proxy. El tráfico del plano de datos se reenvía principalmente en la ruta rápida y nunca se destina al dispositivo Cisco IOS XR local.

Config Resilient Infrastructure Tester

Puede probar la configuración del router para ver si es segura o no con esta herramienta que funciona para varios sistemas operativos, incluido IOS XR: Cisco Config Resilient Infrastructure Tester.

Pregunta y respuesta

1. Si configura un comando por segunda vez o vuelve a configurar el mismo comando, ¿acciona nuevamente el mismo mensaje de advertencia de syslog?

R: No.

2. ¿Causarán dos comandos de configuración para dos funciones diferentes en la misma confirmación dos advertencias de syslog?

R: Yes.

Ejemplo:

RP/0/RP0/CPU0:17 de octubre 19:01:48.806 UTC: ipv6_io[310]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Característica 'IPV6 SOURCE ROUTE' utilizada o configurada. Se sabe que esta función no es segura. Considere la posibilidad de dejar de usarla. No habilite el routing de origen IPv6 debido a riesgos de seguridad.

RP/0/RP0/CPU0:17 de octubre 19:01:48.806 UTC: ipv4_ma[254]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Función 'IPV4 SOURCE ROUTE' utilizada o configurada. Se sabe que esta función no es segura. Considere la posibilidad de dejar de usarla. No habilite el routing de origen IPv4 debido a riesgos de seguridad.

3. ¿Causará una nueva advertencia un nuevo comando de configuración insegura en un nuevo commit?

R: Yes.

4. ¿Hay una advertencia de syslog cuando se elimina la función insegura de la configuración?

R: Yes

Examples:

RP/0/RP0/CPU0:18 de octubre 08:16:24.410 UTC: ssh_conf_proxy[1210]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED: Se ha eliminado la configuración de la función insegura 'algoritmo DSA de clave de host SSH'.

RP/0/RP0/CPU0:22 de octubre 06:37:21.960 UTC: tacacsd[1155]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED: Se ha eliminado la configuración de la función no segura

'Secreto compartido TACACS+ (codificación Tipo 7)'.

RP/0/RP0/CPU0:22 de octubre 06:42:21.805 UTC: tacacsd[1155]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED: Se ha eliminado la configuración de la función 'TACACS+ sobre TCP con secreto compartido (modo predeterminado)'.

5. No verá Telnet disponible en el router.

R: Es posible que ejecute el IOS XR XR7/LNT que tiene Telnet sólo disponible si cargó el RPM de Telnet opcional.

6. No verá que XR7/LNT tenga la opción sFTP o SCP para el comando "install source".

R: En este momento XR7/LNT no soporta sFTP o SCP para el comando "install source".

7. ¿Los cambios se aplican por igual a IOS XR eXR e IOS XR XR7/LNT?

R: Yes.

8. ¿Cómo puede verificar si su router ejecuta IOS XR eXR o IOS XR XR7/LNT?

R: Utilice "show version" y busque "LNT". Los routers 8000 y algunas variantes de NCS540 ejecutan IOS XR XR7/LNT.

Ejemplo:

<#root>

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

Cisco IOS XR Software, Version 25.2.2
LNT
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).