Resiliência da infraestrutura Cisco IOS XR

Contents

Introdução

Este documento descreve um aspecto de proteção do Cisco IOS® XR: eliminar gradualmente recursos e cifras inseguros sistematicamente.

Resiliência da infraestrutura Cisco IOS XR

Para aumentar a postura de segurança dos dispositivos da Cisco, a Cisco está fazendo alterações nas configurações padrão, substituindo e eventualmente removendo recursos não seguros e introduzindo novos recursos de segurança. Essas alterações foram projetadas para fortalecer a infraestrutura da rede e oferecer melhor visibilidade das atividades dos agentes de ameaças.

Consulte esta página da Central de Confiabilidade: Infraestrutura Resiliente. Ele menciona o Endurecimento da infraestrutura, o Guia de endurecimento do software Cisco IOS XR, o processo de reprovação de recursos e os detalhes de reprovação e remoção de recursos. As alternativas sugeridas são mencionadas aqui: Remoção de recursos e Alternativas sugeridas.

O Cisco IOS XR está eliminando progressivamente os recursos e as cifras não confiáveis. Isso inclui os comandos de configuração e execução no Cisco IOS XR.

Recursos afetados

- Telnet
- TFTP
- FTP
- HTTP
- SNMP v1/v2c
- SNMP v3 sem authPriv
- Rota de origem IP
- Servidores pequenos TCP/UDP
- TACACS+ e Radius com chaves pré-compartilhadas (Tipo 7) e MD5
- SSH v1
- TLS 1.0/1.1
- NTPv2/3 e MD5
- GRPC sem TLS, TLSv1.0/1.1
- Executar comandos usando copiar, utilitário e instalar com TFTP/FTP

Agrupamento

Existem comandos de configuração, mas também comandos de execução (por exemplo, o comando "copy").

Os comandos preteridos podem ser agrupados:

- SSHv1, Telnet (servidor e cliente), TFTP (cliente), FTP
- DSA host-key, TACACS/RADIUS Tipo 7, TLS 1.0/1.1
- Outro: Pequenos servidores TCP/UDP, roteamento de origem IP (IPv4 e IPv6)

Fases

Este projeto segue a abordagem usual de substituição de recursos: avisar -> restringir -> remover.

- Avisos no Cisco IOS XR versão 25.4.1.
- Fase de restrição
- Remoção de recursos

Fase de Aviso

Quais são os avisos?

1. A função de ajuda da CLI (Command Line Interface, Interface de Linha de Comando)

2. Um aviso de syslog
3. Um aviso de descrição no módulo yang

Os avisos são emitidos para opções configuradas que não são seguras. Essas são mensagens de syslog com **uma frequência de 30 dias**.

Quando qualquer recurso inseguro é usado, este aviso de log (nível 4 ou aviso) é emitido:

*%**INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN**: Recurso '<feature-name>' utilizado ou configurado. Este recurso é conhecido por ser inseguro. Considere interromper o uso deste recurso. <Recomendação>*

A recomendação é o que usar em vez da opção insegura.

Exemplo de aviso para FTP:

%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Recurso 'FTP' utilizado ou configurado. Este recurso é conhecido por ser inseguro. Considere interromper o uso deste recurso. É recomendável usar o SFTP.

Observe as palavras utilizadas ou configuradas. Utilizado se refere a um comando de execução e configurado se refere a um comando de configuração.

Uma mensagem de aviso pode ser impressa se a opção insegura for removida (nível 6 ou informativo). Exemplo:

RP/0/RP0/CPU0:Oct 22 06:43:43.967 UTC: tacacsd[115]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED : Configuração do recurso inseguro 'TACACS+ sobre TCP com segredo compartilhado (modo padrão)' removida.

Lista de opções inseguras preteridas

Esta é a lista de opções não seguras que acionam um aviso nas versões do Cisco IOS XR da fase de aviso.

A lista mostra a opção insegura, os comandos configuration ou execute, a mensagem de advertência e o modelo Yang associado.

Roteamento de origem 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

Aviso

RP/0/RP0/CPU0:Oct 17 19:01:48.806 UTC: ipv4_ma[254]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Recurso 'ROTA DE ORIGEM IPV4' utilizado ou configurado. Este recurso é conhecido por ser inseguro. Considere interromper o uso deste recurso. Não habilite o roteamento de origem IPv4 devido a riscos de segurança.

RP/0/RP0/CPU0:Oct 17 19:01:48.806 UTC: ipv6_io[310]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Recurso 'ROTA DE ORIGEM IPV6' utilizado ou configurado. Este recurso é conhecido por ser inseguro. Considere interromper o uso deste recurso. Não habilite o roteamento de origem IPv6 devido a riscos de segurança.

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

Recomendação

Remova a opção insegura.

Não existe uma alternativa exata. Os clientes que desejam controlar o tráfego através de uma rede baseada no endereço de origem podem fazê-lo usando o roteamento baseado em políticas ou outros mecanismos de roteamento de origem controlados pelo administrador que não deixam a decisão de roteamento para o usuário 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

Aviso

RP/0/RP0/CPU0:Nov 19 15:20:42.814 UTC: ssh_conf_proxy[1210]: %SECURITY-SSHD_CONF_PRX-4-WARNING_GENERAL : Servidor de backup, configurações de porta netconf, ssh v1, porta ssh não são suportados nesta plataforma e versão, não terão efeito

Modelo Yang

Cisco-IOS-XR-um-ssh-cfg

Recomendação

Use SSH v2.

Configuração SSHv2: Implementação de Secure Shell

TACACS+ e Radius com chaves pré-compartilhadas (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

key 7 1513090F007B7977

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

key 7 1513090F007B7977

aaa server radius dynamic-author

padrão vrf do cliente 10.10.10.2

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

tecla 7 1304464058

Aviso

RP/0/RP0/CPU0:Oct 18 18:00:42.505 UTC: tacacsd[115]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Recurso 'Segredo compartilhado TACACS+ (codificação Tipo 7)' utilizado ou configurado. Este recurso é conhecido por ser inseguro. Considere interromper o uso deste recurso. Em vez disso, use a criptografia Tipo 6 (baseada em AES).

RP/0/RP0/CPU0:Oct 18 18:00:42.505 UTC: tacacsd[115]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Recurso 'TACACS+ sobre TCP com segredo compartilhado (modo padrão)' utilizado ou configurado. Este recurso é conhecido por ser inseguro. Considere interromper o uso deste recurso. Use o TACACS+ sobre TLS (TACACS+ seguro) para uma segurança mais forte.

RP/0/RP0/CPU0:Oct 18 18:18:19.460 UTC: radiusd[1149]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Recurso 'Segredo compartilhado RADIUS (codificação Tipo 7)' utilizado ou configurado. Este recurso é conhecido por ser inseguro. Considere interromper o uso deste recurso. Em vez disso, use a criptografia Tipo 6 (baseada em AES).

RP/0/RP0/CPU0:Oct 18 18:18:19.460 UTC: radiusd[1149]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Recurso 'RADIUS sobre UDP com segredo compartilhado (modo padrão)' utilizado ou configurado. Este recurso é conhecido por ser inseguro. Considere interromper o uso deste recurso. Use RADIUS sobre TLS (RadSec) ou DTLS para obter uma segurança mais forte.

Modelo Yang

-

Recomendação

Use TACACS+ ou Radius sobre TLS 1.3 ou DTLS. Use o Tipo 6 para credenciais.

Configuração de TACACS+ ou Radius sobre TLS 1.3 ou DTLS: Configuração de Serviços AAA

TLS 1.0/1.1, depreciar cifras fracas

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

Aviso

-

Modelo Yang

Cisco-IOS-XR-um-logging-cfg

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

Recomendação

Use TLS1.2 ou TLS1.3.

Configuração Registro Seguro: Implementação de Registro Seguro

Telnet (servidor e 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

Aviso

RP/0/RP0/CPU0:Jun 27 10:59:52.226 UTC: cinetd[145]: %IP-CINETD-4-TELNET_WARNING : O suporte a Telnet está sendo substituído a partir de 25.4.1. Em vez disso, use SSH.

Modelo Yang

Cisco-IOS-XR-ipv4-telnet-cfg

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

Cisco-IOS-XR-um-telnet-cfg

Recomendação

Use SSHv2.

Configuração SSHv2: Implementação de Secure Shell

TFTP (servidor e 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

Aviso

RP/0/RP0/CPU0:17 de outubro 19:03:29.475 UTC: tftp_fs[414]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Recurso 'cliente TFTP' utilizado ou configurado. Este recurso é conhecido por ser inseguro. Considere interromper o uso deste recurso. Em vez disso, use SFTP.

Modelo Yang

-

Recomendação

Use sFTP ou HTTPS.

Configuração sFTP: Implementação de Secure Shell

Servidores pequenos 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

Aviso

-

Modelo Yang

Cisco-IOS-XR-ip-tcp-cfg

Cisco-IOS-XR-ip-udp-cfg

Recomendação

Desabilite servidores pequenos 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

Aviso

RP/0/RP0/CPU0:Oct 16 21:42:42.897 UTC: ftp_fs[190]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Recurso 'cliente FTP' utilizado ou configurado. Este recurso é conhecido por ser inseguro. Considere interromper o uso deste recurso. Em vez disso, use SFTP.

Modelo Yang

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

Recomendação

Use sFTP ou HTTPS.

Configuração sFTP: Implementação 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 <> versão 1|v2c

snmp-server group <> v1|v2c

snmp-server community-map

comunidade snmp

snmp user <> <> v1|v2c

snmp user <> <> v3 auth md5|sha

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

snmp host <> versão 1|v2c

snmp group <> v1|v2c

snmp community-map

Aviso

-

Modelo Yang

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

Recomendação

Usar SNMPv3 com autenticação e criptografia (authPriv).

Configuração do SNMPv3 com autenticação e authPriv: Configuração do Simple Network Management Protocol

NTP Versão 2 e 3 e Autenticação MD5

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 **<>** versão 2|3

ntp peer **<>** versão 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 **<>** **<>**

Aviso

RP/0/RP0/CPU0:Nov 25 16:09:15.422 UTC: ntpd[159]: %IP-IP_NTP-5-CONFIG_NOT_RECOMMENDED : NTPv2 e NTPv3 são preteridos a partir de 25.4.1. Use NTPv4.

RP/0/RP0/CPU0:Nov 25 16:09:15.422 UTC: ntpd[159]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Recurso 'NTP sem autenticação' utilizado ou configurado. Este recurso é conhecido por ser inseguro. Considere interromper o uso deste recurso.

Modelo Yang

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

Recomendação

Use o NTP versão 4 ou uma autenticação diferente do MD5.

Configuração NTP: [Configuração do 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-cipher default|enable|disable (No TLS 1.2, não é seguro quando conjuntos de cifras não seguros são usados após a avaliação das três configurações)

Aviso

RP/0/RP0/CPU0:Nov 29 19:38:30.833 UTC: emsd[112]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Recurso 'gRPC configuração não segura' utilizado ou configurado. Este recurso está obsoleto porque é conhecido por ser inseguro; ele será removido em uma versão futura. server=DEFAULT (a versão do TLS é anterior à 1.2, conjuntos de cifras inseguros estão configurados)

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

Recomendação

Usar TLS 1.2 ou superior (de preferência TLS 1.3) com cifras fortes.

Configuração: Usar Protocolo gRPC para Definir Operações de Rede com Modelos de Dados

Lista de comandos Execute não seguros

Comandos Copy

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 ?"

Aviso

RP/0/RP0/CPU0:Nov 26 15:05:57.666 UTC: filesys_cli[66940]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Recurso 'copy ftp' utilizado ou configurado. Este recurso está obsoleto porque é conhecido por ser inseguro; ele será removido em uma versão futura. Use SFTP ou SCP.

RP/0/RP0/CPU0:Nov 26 15:09:06.181 UTC: filesys_cli[67445]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Recurso 'copy tftp' utilizado ou configurado. Este recurso está obsoleto porque é conhecido por ser inseguro; ele será removido em uma versão futura. Use SFTP ou SCP.

Modelo Yang

-

Recomendação

Use sFTP ou SCP.

Configuração: Implementação de Secure Shell

Comandos de instalação

CLI

```
install source

install add source

install replace

        "
```

Aviso

-

Modelo Yang

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

Recomendação

Use sFTP ou SCP.

Configuração: Implementação de Secure Shell

Comandos do utilitário

CLI

```
utility mv source
```

Modelos Yang

Há muitas mudanças nos modelos Yang para listar todos aqui.

Este é um exemplo para os comentários no *modelo* Yang*Cisco-IOS-XR-ipv4-ma-cfg.*yang para a remoção do roteamento de origem.

```
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 é um exemplo para os comentários no *modelo* Yang *Cisco-IOS-XR-um-ftp-tftp-cfg*.yang para a remoção do FTP e do 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)";
```

Guia de fortalecimento IOS XR

O guia Cisco IOS XR Software Hardening Guide ajuda os administradores de rede e os profissionais de segurança a proteger os roteadores baseados no Cisco IOS XR para aumentar a postura de segurança geral da rede.

Este documento é estruturado em torno dos três planos pelos quais as funções de um dispositivo de rede são categorizadas.

Os três planos funcionais de um roteador são: plano de gerenciamento, plano de controle e plano de dados. Cada um oferece uma funcionalidade diferente que deve ser protegida.

- **Plano de gerenciamento:** o plano de gerenciamento contém o grupo lógico de todo o tráfego que suporta as funções de provisionamento, manutenção e monitoramento para o dispositivo Cisco IOS XR e a rede. O tráfego nesse grupo inclui Secure Shell (SSH), Secure Copy Protocol (SCP), Simple Network Management Protocol (SNMP), Syslog, TACACS+, RADIUS, DNS, NetFlow e Cisco Discovery Protocol. O tráfego do plano de gerenciamento é sempre destinado ao dispositivo Cisco IOS XR local.
- **Plano de Controle:** O plano de controle contém o grupo lógico de todos os protocolos de roteamento, sinalização, link-state e outros protocolos de controle que são usados para criar e manter o estado da rede e suas interfaces. Eles incluem BGP (Border Gateway Protocol), OSPF (Open Shortest Path First), LDP (Label Distribution Protocol), IS-IS (Intermediate System to Intermediate System), NTP (Network Time Protocol), ARP (Address Resolution Protocol) e manutenções de atividades da camada 2. O tráfego do plano de controle é sempre destinado ao dispositivo Cisco IOS XR local.
- **Plano de dados:** o plano de dados contém o grupo lógico de tráfego de aplicativos de "cliente" gerado por hosts, clientes, servidores e aplicativos que são originados de e destinados a outros dispositivos semelhantes suportados pela rede. Os recursos do plano de dados incluem roteamento de origem de IP, broadcast direcionado de IP, redirecionamentos de ICMP, inalcançáveis de ICMP e proxy ARP. O tráfego de plano de dados é encaminhado principalmente no caminho rápido e nunca é destinado ao dispositivo Cisco IOS XR local.

Config Resilient Infrastructure Tester (Avaliador de infraestrutura resiliente de configuração)

Você pode testar a configuração do roteador para ver se ela é segura ou não com esta ferramenta que funciona para vários sistemas operacionais, incluindo IOS XR: Cisco Config Resilient Infrastructure Tester.

Pergunta e resposta

1. Se você configurar um comando pela segunda vez ou configurar o mesmo comando novamente, ele disparará a mesma mensagem de aviso do syslog novamente?

R: No.

2. Dois comandos de configuração para dois recursos diferentes na mesma confirmação causarão dois avisos de syslog?

R: Yes.

Exemplo:

RP/0/RP0/CPU0:Oct 17 19:01:48.806 UTC: ipv6_io[310]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Recurso 'ROTA DE ORIGEM IPV6' utilizado ou configurado. Este recurso é conhecido por ser inseguro. Considere interromper o uso deste recurso. Não habilite o roteamento de origem IPv6 devido a riscos de segurança.

RP/0/RP0/CPU0:Oct 17 19:01:48.806 UTC: ipv4_ma[254]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Recurso 'ROTA DE ORIGEM IPV4' utilizado ou configurado. Este recurso é conhecido por ser inseguro. Considere interromper o uso deste recurso. Não habilite o roteamento de origem IPv4 devido a riscos de segurança.

3. Um novo comando de configuração não seguro em uma nova confirmação causará um novo aviso?

R: Yes.

4. Há um aviso de syslog quando o recurso inseguro é removido da configuração?

R: Yes

Examples:

RP/0/RP0/CPU0:Oct 18 08:16:24.410 UTC: ssh_conf_proxy[1210]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED : Configuração do recurso inseguro 'SSH host-key DSA algorithm' removida.

RP/0/RP0/CPU0:Oct 22 06:37:21.960 UTC: tacacsd[115]: %INFRA-WARN_INSECURE-6-

INSECURE_CONFIG_REMOVED : Configuração do recurso inseguro 'TACACS+ shared secret (codificação Type 7)' removida.

RP/0/RP0/CPU0:Oct 22 06:42:21.805 UTC: tacacsd[115]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED : Configuração do recurso inseguro 'TACACS+ sobre TCP com segredo compartilhado (modo padrão)' removida.

5. Você não vê o Telnet disponível em seu roteador.

R: É possível que você execute o IOS XR XR7/LNT, que tem o Telnet disponível apenas se você tiver carregado o RPM de Telnet opcional.

6. Você não vê XR7/LNT tendo a opção sFTP ou SCP para o comando "install source".

R: Neste momento, XR7/LNT não suporta sFTP ou SCP para o comando "install source".

7. As alterações aplicam-se igualmente ao IOS XR eXR e ao IOS XR XR7/LNT?

R: Yes.

8. Como você pode verificar se o roteador executa IOS XR eXR ou IOS XR XR7/LNT

R: Use "show version" e procure "LNT". Os roteadores 8000 e algumas variantes do NCS540 executam o IOS XR XR7/LNT.

Exemplo:

<#root>

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

Cisco IOS XR Software, Version 25.2.2
LNT
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.