Résilience de l'infrastructure Cisco IOS XR

Table des matières

Introduction

Ce document décrit un aspect du durcissement de Cisco IOS® XR : éliminez systématiquement les fonctions et les chiffrements non sécurisés.

Résilience de l'infrastructure Cisco IOS XR

Pour améliorer la sécurité des périphériques Cisco, Cisco modifie les paramètres par défaut, déprécie et, à terme, supprime les fonctionnalités non sécurisées et introduit de nouvelles fonctionnalités de sécurité. Ces modifications sont conçues pour renforcer votre infrastructure réseau et offrir une meilleure visibilité sur les activités des acteurs de la menace.

Consultez la page Centre de gestion de la confidentialité : Infrastructure résiliente. Il mentionne le durcissement de l'infrastructure, le guide de durcissement du logiciel Cisco IOS XR, le processus

d'annulation de la fonctionnalité et les détails d'annulation et de suppression de la fonctionnalité. Les alternatives suggérées sont mentionnées ici : Suppression de fonctionnalités et Suggestions d'alternatives.

Cisco IOS XR élimine progressivement les fonctions et les chiffrements non sécurisés. Cela inclut les commandes de configuration et d'exécution dans Cisco IOS XR.

Fonctionnalités impactées

- Telnet
- TFTP
- FTP
- HTTP
- SNMP v1/v2c
- SNMP v3 sans authPriv
- Route source IP
- Petits serveurs TCP/UDP
- TACACS+ et Radius avec clés pré-partagées (Type 7) et MD5
- SSH v1
- TLS 1.0/1.1
- NTPv2/3 et MD5
- GRPC no TLS, TLSv1.0/1.1
- Commandes d'exécution avec copy, utility et install avec TFTP/FTP

Regroupement

Il existe des commandes de configuration, mais aussi des commandes d'exécution (par exemple la commande "copy").

Les commandes déconseillées peuvent être regroupées :

- SSHv1, Telnet (serveur et client), TFTP (client), FTP
- DSA host-key, TACACS/RADIUS Type 7, TLS 1.0/1.1
- Divers : Petits serveurs TCP/UDP, routage IP source (IPv4 et IPv6)

Phases

Ce projet suit l'approche habituelle de dépréciation des fonctionnalités : warn -> restrict -> remove.

- Avertissements dans Cisco IOS XR version 25.4.1.
- Phase de restriction
- Suppression de fonctionnalités

Phase D'Avertissement

Quels sont les avertissements ?

1. Fonction d'aide de l'interface de ligne de commande
2. Un avertissement Syslog

3. Un avertissement de description dans le module yang

Des avertissements sont émis pour les options non sécurisées configurées. Il s'agit de messages syslog avec **une fréquence de 30 jours**.

Lorsqu'une fonctionnalité non sécurisée est utilisée, cet avertissement de journal (niveau 4 ou avertissement) est émis :

*%**INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN** : Fonction '<feature-name>' utilisée ou configurée. Cette fonctionnalité est connue pour être non sécurisée, pensez à cesser de l'utiliser. <Recommandation>*

La recommandation est ce qu'il faut utiliser au lieu de l'option non sécurisée.

Exemple d'avertissement pour FTP :

%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Fonction « FTP » utilisée ou configurée. Cette fonctionnalité est connue pour être non sécurisée, pensez à cesser de l'utiliser. Il est recommandé d'utiliser SFTP.

Notez les mots utilisés ou configurés. Utilisé fait référence à une commande d'exécution et configuré fait référence à une commande de configuration.

Un message d'avertissement peut être imprimé si l'option non sécurisée est supprimée (niveau 6 ou informatif). Exemple :

RP/0/RP0/CPU0:Oct 22 06:43:43.967 UTC: tacacsd[1155] : %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED : La configuration de la fonctionnalité non sécurisée « TACACS+ sur TCP avec secret partagé (mode par défaut) » a été supprimée.

Liste des options non sécurisées désapprouvées

Voici la liste des options non sécurisées qui déclenchent un avertissement dans les versions de Cisco IOS XR de la phase d'avertissement.

La liste affiche l'option non sécurisée, les commandes de configuration ou d'exécution, le message d'avertissement et le modèle Yang associé.

Routage source 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

Avertissement

RP/0/RP0/CPU0:Oct 17 19:01:48.806 UTC: ipv4_ma[254] : %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Fonction « IPV4 SOURCE ROUTE » utilisée ou configurée. Cette fonctionnalité est connue pour être non sécurisée, pensez à cesser de l'utiliser. N'activez pas le routage source IPv4 en raison de risques de sécurité.

RP/0/RP0/CPU0:Oct 17 19:01:48.806 UTC: ipv6_io[310] : %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Fonction « IPV6 SOURCE ROUTE » utilisée ou configurée. Cette fonctionnalité est connue pour être non sécurisée, pensez à cesser de l'utiliser. N'activez pas le routage source IPv6 en raison de risques de sécurité.

Modèle 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

Recommandation

Supprimez l'option non sécurisée.

Il n'existe aucune alternative exacte. Les clients qui souhaitent contrôler le trafic via un réseau en fonction de l'adresse source peuvent le faire à l'aide d'un routage basé sur des stratégies ou d'autres mécanismes de routage à la source contrôlés par l'administrateur qui ne laissent pas la décision de routage à l'utilisateur 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

Avertissement

RP/0/RP0/CPU0:Nov 19 15:20:42.814 UTC : ssh_conf_proxy[1210] : %SECURITY-SSHD_CONF_PRX-4-WARNING_GENERAL : Le serveur de sauvegarde, les configurations de port netconf, ssh v1, le port ssh ne sont pas pris en charge dans cette plate-forme et cette version ne prendra pas effet

Modèle Yang

Cisco-IOS-XR-um-ssh-cfg

Recommandation

Utilisez SSH v2.

Configuration SSHv2 : implémentation de Secure Shell

TACACS+ et Radius avec clés pré-partagées (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

clé 7 1513090F007B7977

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

clé 7 1513090F007B7977

serveur aaa radius dynamic-author

client 10.10.10.2 vrf default

server-key 7 05080F1C243

radius-server key 7 130415110F

aaa group server radius RAD

server-private 10.2.4.5 auth-port 12344 acct-port 12345

clé 7 1304464058

Avertissement

RP/0/RP0/CPU0:18 octobre 18:00:42.505 UTC: tacacsd[1155] : %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : La fonctionnalité « secret partagé TACACS+ (codage de type 7) » est utilisée ou configurée. Cette fonctionnalité est connue pour être non sécurisée, pensez à cesser de l'utiliser. Utilisez plutôt le cryptage de type 6 (AES).

RP/0/RP0/CPU0:18 octobre 18:00:42.505 UTC: tacacsd[1155] : %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : La fonctionnalité « TACACS+ sur TCP avec secret partagé (mode par défaut) » est utilisée ou configurée. Cette fonctionnalité est connue pour être non sécurisée, pensez à cesser de l'utiliser. Utilisez TACACS+ sur TLS (Secure TACACS+) pour renforcer la sécurité.

RP/0/RP0/CPU0:Oct 18 18:18:19.460 UTC: radiusd[1149] : %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : La fonctionnalité « secret partagé RADIUS (codage de type 7) » est utilisée ou configurée. Cette fonctionnalité est connue pour être non sécurisée, pensez à cesser de l'utiliser. Utilisez plutôt le cryptage de type 6 (AES).

RP/0/RP0/CPU0:Oct 18 18:18:19.460 UTC: radiusd[1149] : %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : La fonctionnalité « RADIUS sur UDP avec secret partagé (mode par défaut) » est utilisée ou configurée. Cette fonctionnalité est connue pour être non sécurisée, pensez à cesser de l'utiliser. Utilisez RADIUS sur TLS (RadSec) ou DTLS pour renforcer la sécurité.

Modèle Yang

-

Recommandation

Utilisez TACACS+ ou Radius sur TLS 1.3 ou DTLS. Utilisez le type 6 pour les informations d'identification.

Configuration de TACACS+ ou Radius sur TLS 1.3 ou DTLS : Configuration des services AAA

TLS 1.0/1.1, déprécier les chiffrements faibles

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 nom-serveur <> max-version tls1.0|tls1.1

Avertissement

-

Modèle Yang

Cisco-IOS-XR-um-logging-cfg

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

Recommandation

Utilisez TLS1.2 ou TLS1.3.

Configuration de la consignation sécurisée : implémentation de la consignation sécurisée

Telnet (serveur et 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 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

Avertissement

RP/0/RP0/CPU0:Jun 27 10:59:52.226 UTC: cinetd[145] : %IP-CINETD-4-TELNET_WARNING : La prise en charge de Telnet est déconseillée à partir de la version 25.4.1. Veuillez utiliser SSH à la place.

Modèle Yang

Cisco-IOS-XR-ipv4-telnet-cfg

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

Cisco-IOS-XR-um-telnet-cfg

Recommandation

Utilisez SSHv2.

Configuration SSHv2 : implémentation de Secure Shell

TFTP (serveur et 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

client TFTP

Avertissement

RP/0/RP0/CPU0:Oct 17 19:03:29.475 UTC: tftp_fs[414] : %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Fonction « client TFTP » utilisée ou configurée. Cette fonctionnalité est connue pour être non sécurisée, pensez à cesser de l'utiliser. Utilisez plutôt SFTP.

Modèle Yang

-

Recommandation

Utilisez sFTP ou HTTPS.

Configuration sFTP : implémentation de Secure Shell

Petits serveurs 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

Avertissement

-

Modèle Yang

Cisco-IOS-XR-ip-tcp-cfg

Cisco-IOS-XR-ip-udp-cfg

Recommandation

Désactivez les petits serveurs 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

Avertissement

RP/0/RP0/CPU0:Oct 16 21:42:42.897 UTC: ftp_fs[1190] : %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Fonction « client FTP » utilisée ou configurée. Cette fonctionnalité est connue pour être non sécurisée, pensez à cesser de l'utiliser. Utilisez plutôt SFTP.

Modèle Yang

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

Recommandation

Utilisez sFTP ou HTTPS.

Configuration sFTP : implémentation 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

communauté snmp

utilisateur snmp <> <> v1|v2c

snmp user <> <> v3 auth md5|sha

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

snmp host <> version 1|v2c

groupe snmp <> v1|v2c

snmp community-map

Avertissement

-

Modèle Yang

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

Recommandation

Utilisez SNMPv3 avec authentification et cryptage (authPriv).

Configuration de SNMPv3 avec authentification et authPriv : [configuration du protocole SNMP]

Authentification NTP versions 2 et 3 et 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 **<>** 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 **<>** **<>**

Avertissement

RP/0/RP0/CPU0:Nov 25 16:09:15.422 UTC : ntpd[159] : %IP-IP_NTP-5-CONFIG_NOT_RECOMMENDED : NTPv2 et NTPv3 sont déconseillés à partir de 25.4.1. Veuillez utiliser NTPv4.

RP/0/RP0/CPU0:Nov 25 16:09:15.422 UTC : ntpd[159] : %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Fonction « NTP sans authentification » utilisée ou configurée. Cette fonctionnalité est connue pour être non sécurisée, pensez à cesser de l'utiliser.

Modèle Yang

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

Recommandation

Utilisez NTP version 4 ou une authentification autre que MD5.

Configuration NTP : [Configuration du protocole NTP]

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-chiffrement default|enable|disable (dans TLS 1.2, non sécurisé lorsque des suites de chiffrement non sécurisées sont utilisées après l'évaluation des trois configurations)

Avertissement

RP/0/RP0/CPU0:Nov 29 19:38:30.833 UTC : emsd[122] : %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : La fonctionnalité « configuration non sécurisée gRPC » est utilisée ou configurée. Cette fonctionnalité est déconseillée car elle est connue pour être non sécurisée ; il sera supprimé dans une version ultérieure. server=DEFAULT (la version de TLS est antérieure à 1.2, des suites de chiffrement non sécurisées sont configurées)

Modèle 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

Recommandation

Utilisez TLS 1.2 ou supérieur (de préférence TLS 1.3) avec des chiffres forts.

Configuration : utilisation du protocole gRPC pour définir les opérations réseau avec les modèles de données

Liste des commandes d'exécution non sécurisées

Commandes de copie

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 ?"

Avertissement

RP/0/RP0/CPU0:Nov 26 15:05:57.666 UTC : filesys_cli[66940] : %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Fonction « copy ftp » utilisée ou configurée. Cette fonctionnalité est déconseillée car elle est connue pour être non sécurisée ; il sera supprimé dans une version ultérieure. Utilisez plutôt SFTP ou SCP.

RP/0/RP0/CPU0:Nov 26 15:09:06.181 UTC : filesys_cli[67445] : %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Fonction « copy tftp » utilisée ou configurée. Cette fonctionnalité est déconseillée car elle est connue pour être non sécurisée ; il sera supprimé dans une version ultérieure. Utilisez plutôt SFTP ou SCP.

Modèle Yang

-

Recommandation

Utilisez sFTP ou SCP.

Configuration : implémentation de Secure Shell

Commandes d'installation

CLI

```
install source

install add source

install replace

       "
```

Avertissement

-

Modèle Yang

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

Recommandation

Utilisez sFTP ou SCP.

Configuration : implémentation de Secure Shell

Commandes des utilitaires

CLI

```
utility mv source
```

Modèles Yang

Il y a trop de changements dans les modèles Yang pour les lister tous ici.

Il s'agit d'un exemple pour les commentaires dans le *modèle* Yang*Cisco-IOS-XR-ipv4-ma-cfg*.yang pour la suppression du routage source.

```
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)";
```

Ceci est un exemple pour les commentaires dans le *modèle* Yang*Cisco-IOS-XR-um-ftp-tftp-cfg*.yang pour la suppression de FTP et 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)";
```

Guide de renforcement IOS XR

Le guide Cisco IOS XR Software Hardening Guide aide les administrateurs réseau et les professionnels de la sécurité à sécuriser les routeurs basés sur Cisco IOS XR afin d'améliorer la sécurité globale du réseau.

Ce document est structuré autour des trois plans par lesquels les fonctions d'un périphérique réseau sont catégorisées.

Les trois plans fonctionnels d'un routeur sont le plan de gestion, le plan de contrôle et le plan de données. Chacun d'eux fournit une fonctionnalité différente qui doit être protégée.

- **Plan de gestion :** le plan de gestion contient le groupe logique de tout le trafic qui prend en charge les fonctions de mise à disposition, de maintenance et de surveillance du périphérique Cisco IOS XR et du réseau. Le trafic de ce groupe comprend Secure Shell (SSH), Secure Copy Protocol (SCP), Simple Network Management Protocol (SNMP), Syslog, TACACS+, RADIUS, DNS, NetFlow et Cisco Discovery Protocol. Le trafic du plan de gestion est toujours destiné au périphérique Cisco IOS XR local.
- **Plan de contrôle :** le plan de contrôle contient le groupe logique de tous les protocoles de routage, de signalisation, d'état des liaisons et autres protocoles de contrôle utilisés pour créer et maintenir l'état du réseau et de ses interfaces. Il s'agit notamment du protocole BGP (Border Gateway Protocol), de l'OSPF (Open Shortest Path First), du protocole LDP (Label Distribution Protocol), de l'IS-IS (Intermediate System to Intermediate System), du protocole NTP (Network Time Protocol), du protocole ARP (Address Resolution Protocol) et des keepalives de couche 2. Le trafic du plan de contrôle est toujours destiné au périphérique Cisco IOS XR local.

- **Plan de données :** le plan de données contient le groupe logique du trafic d'applications « client » généré par les hôtes, les clients, les serveurs et les applications qui proviennent et sont destinés à d'autres périphériques similaires pris en charge par le réseau. Les fonctions du plan de données incluent le routage de source IP, la diffusion dirigée IP, les redirections ICMP, les ICMP inaccessibles et le proxy ARP. Le trafic du plan de données est principalement transféré sur le chemin rapide et n'est jamais destiné au périphérique Cisco IOS XR local.

Testeur d'infrastructure résiliente de configuration

Vous pouvez tester la configuration du routeur afin de voir s'il est sécurisé ou non avec cet outil qui fonctionne pour plusieurs systèmes d'exploitation, y compris IOS XR : Cisco Config Resilient Infrastructure Tester.

Questions et réponses

1. Si vous configurez une commande la deuxième fois ou si vous reconfigurez la même commande, déclenche-t-elle à nouveau le même message d'avertissement Syslog ?

A : No.

2. Deux commandes de configuration pour deux fonctions différentes dans la même validation provoqueront-elles deux avertissements syslog ?

A : Oui.

Exemple :

RP/0/RP0/CPU0:Oct 17 19:01:48.806 UTC: ipv6_io[310] : %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Fonction « IPV6 SOURCE ROUTE » utilisée ou configurée. Cette fonctionnalité est connue pour être non sécurisée, pensez à cesser de l'utiliser. N'activez pas le routage source IPv6 en raison de risques de sécurité.

RP/0/RP0/CPU0:Oct 17 19:01:48.806 UTC: ipv4_ma[254] : %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN : Fonction « IPV4 SOURCE ROUTE » utilisée ou configurée. Cette fonctionnalité est connue pour être non sécurisée, pensez à cesser de l'utiliser. N'activez pas le routage source IPv4 en raison de risques de sécurité.

3. Une nouvelle commande de configuration non sécurisée dans une nouvelle validation provoquera-t-elle un nouvel avertissement ?

A : Oui.

4. Y a-t-il un avertissement syslog lorsque la fonctionnalité non sécurisée est supprimée de la configuration ?

A : Oui

Exemples:

RP/0/RP0/CPU0:Oct 18 08:16:24.410 UTC: ssh_conf_proxy[1210] : %INFRA-WARN_INSECURE-

6-INSECURE_CONFIG_REMOVED : La configuration de la fonction non sécurisée « SSH host-key DSA algorithm » a été supprimée.

RP/0/RP0/CPU0:Oct 22 06:37:21.960 UTC: tacacsd[1155] : %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED : La configuration de la fonctionnalité non sécurisée « TACACS+ secret partagé (codage de type 7) » a été supprimée.

RP/0/RP0/CPU0:Oct 22 06:42:21.805 UTC: tacacsd[1155] : %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED : La configuration de la fonctionnalité non sécurisée « TACACS+ sur TCP avec secret partagé (mode par défaut) » a été supprimée.

5. Vous ne voyez pas Telnet disponible sur votre routeur.

A : Il est possible que vous exécutiez IOS XR XR7/LNT qui dispose de Telnet uniquement si vous avez chargé le RPM Telnet facultatif.

6. Vous ne voyez pas XR7/LNT ayant l'option sFTP ou SCP pour la commande « install source ».

A : Actuellement, XR7/LNT ne prend pas en charge sFTP ou SCP pour la commande « install source ».

7. Les modifications s’appliquent-elles également à IOS XR eXR et à IOS XR XR7/LNT ?

A : Oui.

8. Comment vérifier si votre routeur exécute IOS XR eXR ou IOS XR XR7/LNT ?

A : Utilisez « show version » et recherchez « LNT ». Les routeurs 8000 et certaines variantes de NCS540 exécutent IOS XR XR7/LNT.

Exemple :

<#root>

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

Cisco IOS XR Software, Version 25.2.2
LNT
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.