Resilienza dell'infrastruttura Cisco IOS XR

Sommario

- Introduzione
- Resilienza dell'infrastruttura Cisco IOS XR
  - Caratteristiche interessate
  - Raggruppamento
    - Fasi
  - Fase di avvertenza
  - Elenco delle opzioni non sicure obsolete
    - RFC 791 (IP source routing)
    - SSH v1
    - TACACS+ e Radius con chiavi già condivise (Tipo 7)
    - TLS 1.0/1.1, deprecazione dei cifrari deboli
    - Telnet (server e client)
    - TFTP (server e client)
    - Server di piccole dimensioni TCP/UDP
    - FTP
    - SNMP v1/2c
    - Autenticazione NTP versione 2 e 3 e MD5
    - GRPC
  - Elenco dei comandi Execute non sicuri
    - Comandi Copy
    - Comandi di installazione
    - Comandi di utilità
  - Modelli Yang
- Guida alla protezione avanzata di IOS XR
- Config Resilient Infrastructure Tester
- Domanda e risposta

Introduzione

Questo documento descrive un aspetto della protezione avanzata di Cisco IOS® XR: eliminare gradualmente le funzioni e i cifrari non sicuri in modo sistematico.

Resilienza dell'infrastruttura Cisco IOS XR

Per aumentare la postura di sicurezza dei dispositivi Cisco, Cisco sta modificando le impostazioni predefinite, deprecando ed eventualmente rimuovendo le funzionalità non sicure, e introducendo nuove funzionalità di sicurezza. Queste modifiche sono progettate per rafforzare l'infrastruttura di rete e fornire una migliore visibilità sulle attività degli attori della minaccia.

Consultare la pagina Centro protezione: Infrastruttura resiliente. Vengono descritti la protezione avanzata dell'infrastruttura, la guida alla protezione avanzata del software Cisco IOS XR, il

processo di deprecazione delle funzionalità e i dettagli relativi all'obsolescenza e alla rimozione delle funzionalità. Le alternative suggerite sono indicate di seguito: rimozione delle funzionalità e alternative suggerite.

Cisco IOS XR sta eliminando funzionalità e cifrari non sicuri. Sono inclusi sia i comandi di configurazione che quelli di esecuzione in Cisco IOS XR.

Caratteristiche interessate

- Telnet
- TFTP
- FTP
- HTTP
- SNMP v1/v2c
- SNMP v3 senza authPriv
- Route di origine IP
- Piccoli server TCP/UDP
- TACACS+ e Radius con chiavi già condivise (Tipo 7) e MD5
- SSH v1
- TLS 1.0/1.1
- NTPv2/3 e MD5
- GRPC senza TLS, TLSv1.0/1.1
- Eseguire i comandi utilizzando copy, utility e install con TFTP/FTP

Raggruppamento

Sono disponibili alcuni comandi di configurazione, ma anche di esecuzione (ad esempio il comando "copy").

I comandi deprecati possono essere raggruppati:

- SSHv1, Telnet (server e client), TFTP (client), FTP
- Chiave host DSA, TACACS/RADIUS tipo 7, TLS 1.0/1.1
- Altro: Piccoli server TCP/UDP, routing all'origine IP (IPv4 e IPv6)

Fasi

Questo progetto segue il consueto approccio basato sull'obsolescenza delle caratteristiche: warn -> restrict -> remove (avvisa > limita -> rimuovi).

- Avvisi in Cisco IOS XR release 25.4.1.
- Fase di restrizione
- Rimozione delle feature

Fase di avvertenza

Quali sono gli avvisi?

1. Funzione della guida CLI (Command Line Interface)
2. Avviso syslog
3. Avviso di descrizione nel modulo Yang

Vengono emessi avvisi per le opzioni non sicure configurate. Si tratta di messaggi syslog con **una frequenza di 30 giorni**.

Quando si usa una funzione non sicura, viene emesso questo messaggio (livello 4 o avviso):

*%**INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN**: Funzionalità '<nome-funzionalità>' utilizzata o configurata. Questa funzionalità è nota come non sicura. Provare a terminare l'utilizzo della funzionalità. <Consiglio>*

Si consiglia di utilizzare l'opzione anziché l'opzione non protetta.

Avviso di esempio per FTP:

%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Funzionalità 'FTP' utilizzata o configurata. Questa funzionalità è nota come non sicura. Provare a terminare l'utilizzo della funzionalità. Si consiglia di utilizzare SFTP.

Osservate le parole utilizzate o configurate. Utilizzato fa riferimento a un comando di esecuzione e configurato fa riferimento a un comando di configurazione.

Se l'opzione non protetta viene rimossa (livello 6 o informativo), è possibile stampare un messaggio di avviso. Esempio:

RP/0/RP0/CPU0:ott 22 06:43:43.967 UTC: tacacsd[115]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVAL: La configurazione della funzionalità 'TACACS+ over TCP con shared secret (modalità predefinita)' non è protetta è stata rimossa.

Elenco delle opzioni non sicure obsolete

Di seguito sono elencate le opzioni non sicure che attivano un avviso nelle versioni Cisco IOS XR della fase di avviso.

L'elenco mostra l'opzione non protetta, i comandi di configurazione o esecuzione, il messaggio di avvertenza e il modello Yang associato.

RFC 791 (IP source routing)

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

route di origine ipv6

ipv4 source-route

Avviso

RP/0/RP0/CPU0:ott 17 19:01:48.806 UTC: ipv4_ma[254]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Funzione 'IPV4 SOURCE ROUTE' utilizzata o configurata. Questa funzionalità è nota come non sicura. Provare a terminare l'utilizzo della funzionalità. Non abilitare il routing dell'origine IPv4 a causa di rischi di sicurezza.

RP/0/RP0/CPU0:ott 17 19:01:48.806 UTC: ipv6_io[30]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Funzionalità 'IPV6 SOURCE ROUTE' utilizzata o configurata. Questa funzionalità è nota come non sicura. Provare a terminare l'utilizzo della funzionalità. Non abilitare il routing di origine IPv6 a causa di rischi di protezione.

Modello 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

Suggerimento

Rimuovere l'opzione non protetta.

Non esistono alternative esatte. I clienti che desiderano controllare il traffico attraverso una rete in base all'indirizzo di origine possono farlo utilizzando il routing basato su criteri o altri meccanismi di routing all'origine controllati dall'amministratore che non lasciano la decisione di routing all'utente finale.

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.
```

client ssh v1

server ssh v1

Avviso

RP/0/RP0/CPU0:Nov 19 15:20:42.814 UTC: ssh_conf_proxy[1210]: %SECURITY-SSHD_CONF_PRX-4-WARNING_GENERAL: Il server di backup, le configurazioni delle porte netconf, la porta ssh v1 e la porta ssh non sono supportati in questa piattaforma e versione, non saranno effettivi

Modello Yang

Cisco-IOS-XR-um-ssh-cfg

Suggerimento

Utilizzare SSH v2.

Configurazione SSHv2: implementazione di Secure Shell

TACACS+ e Radius con chiavi già condivise (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.
```

Chiave tacacs-server 7 135445410615102B28252B203E270A

porta 49 dell'host tacacs-server 10.1.1.1

7 1513090F007B7977

host radius-server 10.0.0.1 porta auth 999 porta acct 8888

7 1513090F007B7977

autore dinamico radius server aaa

client 10.10.10.2 vrf default

tasto server 7 05080F1C2243

chiave radius-server 7 130415110F

rad radius server di gruppo aaa

server-private 10.2.4.5 porta auth 12344 porta acct 12345

chiave 7 1304464058

Avviso

RP/0/RP0/CPU0:18 ott 18:00:42,505 UTC: tacacsd[115]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Funzione 'TACACS+ shared secret (codifica tipo 7)' utilizzata o configurata. Questa funzionalità è nota come non sicura. Provare a terminare l'utilizzo della funzionalità. Utilizzare la crittografia di tipo 6 (basata su AES).

RP/0/RP0/CPU0:18 ott 18:00:42,505 UTC: tacacsd[115]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Viene utilizzata o configurata la funzionalità 'TACACS+ over TCP con segreto condiviso (modalità predefinita)'. Questa funzionalità è nota come non sicura. Provare a terminare l'utilizzo della funzionalità. Per una maggiore sicurezza, usare TACACS+ over TLS (Secure TACACS+).

RP/0/RP0/CPU0:ott 18 18:18:19.460 UTC: radiusd[1149]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Funzionalità 'Segreto condiviso RADIUS (codifica tipo 7)' utilizzata o configurata. Questa funzionalità è nota come non sicura. Provare a terminare l'utilizzo della funzionalità. Utilizzare la crittografia di tipo 6 (basata su AES).

RP/0/RP0/CPU0:ott 18 18:18:19.460 UTC: radiusd[1149]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: La funzionalità 'RADIUS over UDP con segreto condiviso (modalità predefinita)' è utilizzata o configurata. Questa funzionalità è nota come non sicura. Provare a terminare l'utilizzo della funzionalità. Per una maggiore sicurezza, utilizzare RADIUS over TLS (RadSec) o DTLS.

Modello Yang

-

Suggerimento

Usare TACACS+ o Radius su TLS 1.3 o DTLS. Utilizzare il tipo 6 per le credenziali.

Configurazione di TACACS+ o Radius su TLS 1.3 o DTLS: configurazione dei servizi AAA

TLS 1.0/1.1, deprecazione dei cifrari deboli

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
```

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

Avviso

-

Modello Yang

Cisco-IOS-XR-um-logging-cfg

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

Suggerimento

Utilizzare TLS1.2 o TLS1.3.

Configuration Secure Logging: implementazione della registrazione sicura

Telnet (server e 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

Avviso

RP/0/RP0/CPU0:Giu 27 10:59:52.226 UTC: cinetd[145]: %IP-CINETD-4-TELNET_WARNING : Il supporto Telnet è obsoleto a partire dalla versione 25.4.1. Usare SSH.

Modello Yang

Cisco-IOS-XR-ipv4-telnet-cfg

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

Cisco-IOS-XR-um-telnet-cfg

Suggerimento

Usare SSHv2.

Configurazione SSHv2: implementazione di Secure Shell

TFTP (server e 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

Avviso

RP/0/RP0/CPU0:17 ott 19:03:29.475 UTC: tftp_fs[414]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Funzione 'client TFTP' utilizzata o configurata. Questa funzionalità è nota come non sicura. Provare a terminare l'utilizzo della funzionalità. Usate SFTP.

Modello Yang

-

Suggerimento

Utilizzare sFTP o HTTPS.

Configuration sFTP: implementazione di Secure Shell

Server di piccole dimensioni 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

servizio ipv6

Avviso

-

Modello Yang

Cisco-IOS-XR-ip-tcp-cfg

Cisco-IOS-XR-ip-udp-cfg

Suggerimento

Disabilitare i server TCP/UDP di piccole dimensioni.

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

Avviso

RP/0/RP0/CPU0:16 ott 21:42:42.897 UTC: ftp_fs[1190]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Funzionalità 'FTP client' utilizzata o configurata. Questa funzionalità è nota come non sicura. Provare a terminare l'utilizzo della funzionalità. Usate SFTP.

Modello Yang

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

Suggerimento

Utilizzare sFTP o HTTPS.

Configuration sFTP: implementazione di 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)
```

community snmp-server

utente snmp-server <> <> v1 | v2c

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

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

host snmp-server <> versione 1|v2c

gruppo snmp-server <> v1|v2c

snmp-server community-map

community snmp

utente snmp <> <> v1|v2c

utente snmp <> <> v3 auth md5|sha

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

host snmp <> versione 1|v2c

snmp group <> v1|v2c

snmp community-map

Avviso

-

Modello Yang

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

Suggerimento

Utilizzare SNMPv3 con autenticazione e crittografia (authPriv).

Configurazione di SNMPv3 con autenticazione e authPriv: configurazione di Simple Network Management Protocol

Autenticazione NTP versione 2 e 3 e 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
```

server ntp **<>** versione 2|3

ntp peer **<>** versione 2/3

admin-plane versione 1/2/3 server ntp

broadcast interface ntp **<>** versione 2|3

ntp interface **<>** multicast versione 2|3

chiave di autenticazione ntp **<>** md5 **<>** **<>**

Avviso

RP/0/RP0/CPU0:Nov 25 16:09:15.42 UTC: ntpd[159]: %IP-IP_NTP-5-CONFIG_NOT_RECOMMENDED : NTPv2 e NTPv3 sono obsoleti a partire dalla versione 25.4.1. Utilizzare NTPv4.

RP/0/RP0/CPU0:Nov 25 16:09:15.42 UTC: ntpd[159]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Funzionalità 'NTP senza autenticazione' utilizzata o configurata. Questa funzionalità è nota come non sicura. Provare a terminare l'utilizzo della funzionalità.

Modello Yang

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

Suggerimento

Utilizzare NTP versione 4 o un'autenticazione diversa da MD5.

Configurazione NTP: [configurazione di 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|versione min 1.0|1.1
grpc tls-cipper default|enable|disable (in TLS 1.2, non sicuro quando vengono usate suite di cifratura non sicure dopo la valutazione delle tre configurazioni)

Avviso

RP/0/RP0/CPU0:Nov 29 19:38:30.83 UTC: emsd[112]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Funzionalità 'configurazione RPC non protetta' utilizzata o configurata. Questa funzionalità è obsoleta perché è nota per essere non sicura. sarà rimosso in una versione futura. server=DEFAULT (la versione TLS è precedente alla 1.2, sono configurate suite di cifratura non sicure)

Modello 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

Suggerimento

Usare TLS 1.2 o versione successiva (preferibilmente TLS 1.3) con cifratura forte.

Configurazione: utilizzare il protocollo RPC per definire le operazioni di rete con i modelli dati

Elenco dei comandi Execute non sicuri

Comandi 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?"

Avviso

RP/0/RP0/CPU0:Nov 26 15:05:57.66 UTC: filesys_cli[6940]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Funzione 'copy ftp' utilizzata o configurata. Questa funzionalità è obsoleta perché è nota per essere non sicura. sarà rimosso in una versione futura. Utilizzare SFTP o SCP.

RP/0/RP0/CPU0:Nov 26 15:09:06.181 UTC: filesys_cli[6745]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Funzione 'copy tftp' utilizzata o configurata. Questa funzionalità è obsoleta perché è nota per essere non sicura. sarà rimosso in una versione futura. Utilizzare SFTP o SCP.

Modello Yang

-

Suggerimento

Utilizzare sFTP o SCP.

Configurazione: implementazione di Secure Shell

Comandi di installazione

CLI

```
install source

install add source

install replace

        "
```

Avviso

-

Modello Yang

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

Suggerimento

Utilizzare sFTP o SCP.

Configurazione: implementazione di Secure Shell

Comandi di utilità

CLI

```
utility mv source
```

Modelli Yang

Ci sono troppi cambiamenti nei modelli Yang per elencarli tutti qui.

Questo è un esempio di commenti nel *modello* Yang *Cisco-IOS-XR-ipv4-ma-cfg*.yang per la rimozione del routing di origine.

```
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)";
```

Questo è un esempio di commenti nel *modello* Yang *Cisco-IOS-XR-um-ftp-tftp-cfg*.yang per la rimozione di FTP e 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)";
```

Guida alla protezione avanzata di IOS XR

La guida alla protezione avanzata del software Cisco IOS XR aiuta gli amministratori di rete e gli operatori di sicurezza a proteggere i router basati su Cisco IOS XR per aumentare la postura di sicurezza complessiva della rete.

Questo documento è strutturato su tre piani in base ai quali sono categorizzate le funzioni di un dispositivo di rete.

I tre piani funzionali di un router sono il piano di gestione, il piano di controllo e il piano dati. Ognuno di essi fornisce una funzionalità diversa che deve essere protetta.

- **Piano di gestione:** il piano di gestione contiene il gruppo logico di tutto il traffico che supporta le funzioni di provisioning, manutenzione e monitoraggio per il dispositivo Cisco IOS XR e la rete. Il traffico in questo gruppo include Secure Shell (SSH), Secure Copy Protocol (SCP), Simple Network Management Protocol (SNMP), Syslog, TACACS+, RADIUS, DNS, NetFlow e il protocollo Cisco Discovery. Il traffico del piano di gestione è sempre destinato al dispositivo Cisco IOS XR locale.
- **Piano di controllo:** il piano di controllo contiene il gruppo logico di tutti i protocolli di routing, segnalazione, stato del collegamento e altri protocolli di controllo utilizzati per creare e mantenere lo stato della rete e delle relative interfacce. tra cui Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), Label Distribution Protocol (LDP), Intermediate System to Intermediate System (IS-IS), Network Time Protocol (NTP), Address Resolution Protocol (ARP) e i pacchetti keepalive di layer 2. Il traffico del control plane è sempre destinato al dispositivo Cisco IOS XR locale.
- **Piano dati:** il piano dati contiene il gruppo logico di traffico di applicazioni "cliente" generato da host, client, server e applicazioni provenienti e destinati ad altri dispositivi simili supportati dalla rete. Le funzionalità del piano dati includono routing di origine IP, broadcast diretto IP, reindirizzamenti ICMP, ICMP "unreachables" e proxy ARP. Il traffico del data plane viene inoltrato principalmente nel percorso rapido e non è mai destinato al dispositivo Cisco IOS XR locale.

Config Resilient Infrastructure Tester

È possibile verificare la configurazione del router per verificare se è sicura o meno con questo strumento, che funziona per diversi sistemi operativi, tra cui IOS XR: Cisco Config Resilient Infrastructure Tester.

Domanda e risposta

1. Se si configura un comando la seconda volta o si configura di nuovo lo stesso comando, viene nuovamente generato lo stesso messaggio di avviso syslog?

A: No.

2. Due comandi di configurazione per due diverse funzionalità nello stesso commit generano due avvisi syslog?

A: Sì.

Esempio:

RP/0/RP0/CPU0:ott 17 19:01:48.806 UTC: ipv6_io[30]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Funzionalità 'IPV6 SOURCE ROUTE' utilizzata o configurata. Questa funzionalità è nota come non sicura. Provare a terminare l'utilizzo della funzionalità. Non abilitare il routing di origine IPv6 a causa di rischi di protezione.

RP/0/RP0/CPU0:ott 17 19:01:48.806 UTC: ipv4_ma[254]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Funzione 'IPV4 SOURCE ROUTE' utilizzata o configurata. Questa funzionalità è nota come non sicura. Provare a terminare l'utilizzo della funzionalità. Non abilitare il routing dell'origine IPv4 a causa di rischi di sicurezza.

3. Un nuovo comando di configurazione non sicura in un nuovo commit genererà un nuovo avviso?

A: Sì.

4. È presente un avviso syslog quando la funzione non sicura viene rimossa dalla configurazione?

A: Sì

Esempi:

RP/0/RP0/CPU0:18 08:16:24.410 UTC: ssh_conf_proxy[1210]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVAL: La configurazione della funzionalità 'SSH host-key DSA algorithm' non protetta è stata rimossa.

RP/0/RP0/CPU0:ott 22 06:37:21.960 UTC: tacacsd[115]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVAL: La configurazione della funzionalità 'TACACS+ shared secret

(codifica tipo 7)' non è protetta è stata rimossa.

RP/0/RP0/CPU0:ott 22 06:42:21.805 UTC: tacacsd[115]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVAL: La configurazione della funzionalità 'TACACS+ over TCP con shared secret (modalità predefinita)' non è protetta è stata rimossa.

5. Telnet non è disponibile sul router.

A: È possibile eseguire IOS XR XR7/LNT con Telnet disponibile solo se è stato caricato il modulo RPM Telnet opzionale.

6. XR7/LNT non dispone dell'opzione sFTP o SCP per il comando "install source".

A: Attualmente XR7/LNT non supporta sFTP o SCP per il comando "install source".

7. Le modifiche sono valide anche per IOS XR eXR e IOS XR XR7/LNT?

A: Sì.

8. Come verificare se il router esegue IOS XR eXR o IOS XR XR7/LNT?

A: Usare "show version" e cercare "LNT". 8000 router e alcune varianti di NCS540 eseguono IOS XR XR7/LNT.

Esempio:

<#root>

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

Cisco IOS XR Software, Version 25.2.2
LNT
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).