Infrastructuur veerkracht Cisco IOS XR

Inhoud

Inleiding

In dit document wordt één aspect van Cisco IOS® XR beschreven: onveilige functies en cijfers worden systematisch uitgefaseerd.

Cisco IOS XR Infrastructure Resilience

Om de beveiligingsstatus van Cisco-apparaten te verhogen, wijzigt Cisco de standaardinstellingen, verlaagt en verwijdert het uiteindelijk onveilige mogelijkheden en introduceert het nieuwe beveiligingsfuncties. Deze wijzigingen zijn bedoeld om uw netwerkinfrastructuur te versterken en een beter inzicht te bieden in activiteiten van bedreigingsactoren.

Kijk maar eens op deze pagina van het Trust Center: Resilient Infrastructure. Het vermeldt de

Infrastructure Hardening, de Cisco IOS XR Software Hardening Guide, de functie afschrijving proces, en functie afschrijving en verwijdering details. De voorgestelde alternatieven worden hier genoemd: Verwijdering van functies en voorgestelde alternatieven.

Cisco IOS XR is het uitfaseren van onveilige functies en cijfers. Dit omvat zowel configuratie- als uitvoeringsopdrachten in Cisco IOS XR.

Geïmpacteerde kenmerken

- Telnet
- TFTP
- FTP
- HTTP
- SNMP v1/v2c
- SNMP v3 zonder authPriv
- IP-bronroute
- Kleine TCP/UDP-servers
- TACACS+ en Radius met vooraf gedeelde sleutels (type 7) en MD5
- SSH v1
- TLS 1,0/1,1
- NTPv2/3 en MD5
- GRPC geen TLS, TLSv1.0/1.1
- Exec-opdrachten met kopiëren, hulpprogramma en installeren met TFTP/FTP

groepering

Er zijn configuratieopdrachten, maar ook uitvoeringsopdrachten (bijvoorbeeld de opdracht "kopiëren").

De opgegeven opdrachten kunnen worden gegroepeerd:

- SSHv1, Telnet (server en client), TFTP (client), FTP
- DSA-host-key, TACACS/RADIUS Type 7, TLS 1.0/1.1
- Overige: TCP/UDP kleine servers, IP-bronroutering (IPv4 en IPv6)

Fasen

Dit project volgt de gebruikelijke afschrijvingsmethode voor functies: waarschuw -> beperk -> verwijder.

- Waarschuwingen in Cisco IOS XR versie 25.4.1.
- Beperkingsfase
- Kenmerken verwijderen

waarschuwingsfase

Wat zijn de waarschuwingen?

1. De helpfunctie CLI (Command Line Interface)
2. Een syslog-waarschuwing
3. Een waarschuwing in de Yang-module

Waarschuwingen worden afgegeven voor geconfigureerde onveilige opties. Dit zijn syslog berichten met **een frequentie van 30 dagen**.

Wanneer een onveilige functie wordt gebruikt, wordt deze logwaarschuwing (niveau 4 of waarschuwing) uitgezonden:

*%**INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN**: Functie '<feature-name>' gebruikt of geconfigureerd. Deze functie staat bekend als onveilig, overweeg het gebruik van deze functie te staken. <Aanbeveling>*

De aanbeveling is wat te gebruiken in plaats van de onzekere optie.

Voorbeeldwaarschuwing voor FTP:

%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Functie 'FTP' gebruikt of geconfigureerd. Deze functie staat bekend als onveilig, overweeg het gebruik van deze functie te staken. Gebruik SFTP.

Let op de gebruikte of geconfigureerde woorden. Utilized verwijst naar een execute commando en configured verwijst naar een configuratie commando.

Een waarschuwingsbericht kan worden afgedrukt als de onveilige optie wordt verwijderd (niveau 6 of informatief). Voorbeeld:

RP/0/RP0/CPU0:Oct 22 06:43:43.967 UTC: tacacsd[1155]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED: Onveilige functie 'TACACS+ over TCP met gedeelde geheime (standaardmodus)' configuratie verwijderd.

Lijst van afgekeurde onveilige opties

Dit is de lijst met onveilige opties die een waarschuwing activeren in Cisco IOS XR-releases van de waarschuwingsfase.

De lijst toont de onveilige optie, de configuratie of het uitvoeren van opdrachten, het waarschuwingsbericht en het bijbehorende Yang-model.

IP-bronrouting (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-bronroute

IPv6-bronroute

IPv4-bronroute

WAARSCHUWING

RP/0/RP0/CPU0:17 okt 19:01:48.806 UTC: ipv4_ma[254]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Kenmerk 'IPV4 SOURCE ROUTE' gebruikt of geconfigureerd. Deze functie staat bekend als onveilig, overweeg het gebruik van deze functie te staken. Schakel IPv4-bronroutering niet in vanwege beveiligingsrisico's.

RP/0/RP0/CPU0:17 okt 19:01:48.806 UTC: ipv6_io[310]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Kenmerk 'IPV6 SOURCE ROUTE' gebruikt of geconfigureerd. Deze functie staat bekend als onveilig, overweeg het gebruik van deze functie te staken. Schakel IPv6-bronroutering niet in vanwege beveiligingsrisico's.

Yang-model

Cisco-IOS-XR-ipv4-ma-cfg

Cisco-IOS-XR-ipv6-io-cfg

Cisco-IOS-XR-um-ipv4-cfg

Cisco-IOS-XR-um-ipv6-cfg

Aanbeveling

Verwijder de onveilige optie.

Er bestaat geen exact alternatief. Klanten die het verkeer via een netwerk willen regelen op basis van het bronadres, kunnen dit doen met behulp van op beleid gebaseerde routering of andere door de beheerder gecontroleerde bronrouteringsmechanismen die de routeringsbeslissing niet aan de eindgebruiker overlaten.

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

WAARSCHUWING

RP/0/RP0/CPU0:19 nov 15:20:42.814 UTC: ssh_conf_proxy[1210]: %SECURITY-SSHD_CONF_PRX-4-WARNING_GENERAL: Back-upserver, netconf-poortconfiguraties, ssh v1, ssh-poort worden niet ondersteund in dit platform en release, wordt niet van kracht

Yang-model

Cisco-IOS-XR-um-ssh-cfg

Aanbeveling

Gebruik SSH v2.

Configuratie SSHv2: implementatie van Secure Shell

TACACS+ en Radius met vooraf gedeelde sleutels (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-serversleutel 7 135445410615102B28252B203E270A

TACACS-serverhost 10.1.1.1 poort 49

sleutel 7 1513090F007B7977

RADIUS-SERVERHOST 10.0.0.1 AUTH-POORT 9999 ACCT-POORT 8888

sleutel 7 1513090F007B7977

AAA Server Radius Dynamic-Author

Client 10.10.10.2 VRF-standaard

server-key 7 05080F1C2243

radius-server sleutel 7 130415110F

radius van aaa-groepsserver RAD

Server-Private 10.2.4.5 Auth-Port 12344 ACCT-Port 12345

Verdeelsleutel 7 1304464058

WAARSCHUWING

RP/0/RP0/CPU0:18 okt 18:00:42.505 UTC: tacacsd[1155]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Kenmerk 'TACACS+ shared secret (Type 7 encoding)' gebruikt of geconfigureerd. Deze functie staat bekend als onveilig, overweeg het gebruik van deze functie te staken. Gebruik in plaats daarvan Type 6 (AES-gebaseerde) codering.

RP/0/RP0/CPU0:18 okt 18:00:42.505 UTC: tacacsd[1155]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Functie 'TACACS+ over TCP met gedeeld geheim (standaardmodus)' gebruikt of geconfigureerd. Deze functie staat bekend als onveilig, overweeg het gebruik van deze functie te staken. Gebruik TACACS+ over TLS (Secure TACACS+) voor een betere beveiliging.

RP/0/RP0/CPU0:Oct 18 18:18:19.460 UTC: radiusd[1149]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Functie 'RADIUS shared secret (Type 7 encoding)' gebruikt of geconfigureerd. Deze functie staat bekend als onveilig, overweeg het gebruik van deze functie te staken. Gebruik in plaats daarvan Type 6 (AES-gebaseerde) codering.

RP/0/RP0/CPU0:18 oktober 18:18:19.460 UTC: radiusd[1149]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Functie 'RADIUS over UDP met gedeeld geheim (standaardmodus)' gebruikt of geconfigureerd. Deze functie staat bekend als onveilig, overweeg het gebruik van deze functie te staken. Gebruik RADIUS over TLS (RadSec) of DTLS voor een betere beveiliging.

Yang-model

-

Aanbeveling

Gebruik TACACS+ of Radius over TLS 1.3 of DTLS. Gebruik Type 6 voor referenties.

Configuratie TACACS+ of Radius over TLS 1.3 of DTLS: AAA-services configureren

TLS 1.0/1.1, zwakke cijfers afkeuren

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
```

Logboekregistratie TLS-servernaam <> MAX-versie TLS1.0|TLS1.1

WAARSCHUWING

-

Yang-model

Cisco-IOS-XR-um-logging-cfg

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

Aanbeveling

Gebruik TLS1.2 of TLS1.3.

Configuration Secure Logging: implementeren van veilige logboekregistratie

Telnet (server en 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

WAARSCHUWING

RP/0/RP0/CPU0:Jun 27 10:59:52.226 UTC: cinetd[145]: %IP-CINETD-4-TELNET_WAARSCHUWING: Telnet-ondersteuning wordt vanaf 25.4.1 afgeschreven. Gebruik in plaats daarvan SSH.

Yang-model

Cisco-IOS-XR-ipv4-telnet-cfg

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

Cisco-IOS-XR-um-telnet-cfg

Aanbeveling

Gebruik SSHv2.

Configuratie SSHv2: implementatie van Secure Shell

TFTP (server en client)

CLI

<#root>

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

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

tftp

IP TFTP

TFTP-client

WAARSCHUWING

RP/0/RP0/CPU0:17 okt 19:03:29.475 UTC: tftp_fs[414]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Functie 'TFTP-client' gebruikt of geconfigureerd. Deze functie staat bekend als onveilig, overweeg het gebruik van deze functie te staken. Gebruik in plaats daarvan SFTP.

Yang-model

-

Aanbeveling

Gebruik sFTP of HTTPS.

Configuratie sFTP: implementeren van Secure Shell

TCP/UDP-kleine servers

CLI

<#root>

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

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

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

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

IPv4-service

IPv6-service

WAARSCHUWING

-

Yang-model

Cisco-IOS-XR-ip-tcp-cfg

Cisco-IOS-XR-ip-udp-cfg

Aanbeveling

Schakel kleine TCP/UDP-servers uit.

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

WAARSCHUWING

RP/0/RP0/CPU0:Oct 16 21:42:42.897 UTC: ftp_fs[1190]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Kenmerk 'FTP-client' gebruikt of geconfigureerd. Deze functie staat bekend als onveilig, overweeg het gebruik van deze functie te staken. Gebruik in plaats daarvan SFTP.

Yang-model

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

Aanbeveling

Gebruik sFTP of HTTPS.

Configuratie sFTP: implementeren van 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-servercommunity

SNMP-servergebruiker <> <> v1 | v2c

SNMP-servergebruiker <> <> v3 Auth MD5 | SHA

SNMP-servergebruiker <> <> v3 auth MD5|SHA <> Priv 3DES|DES56

SNMP-server-host <> versie 1|V2C

SNMP-servergroep <> v1|v2c

SNMP-server community-map

SNMP-community

SNMP-gebruiker <> <> v1|v2c

SNMP-gebruiker <> <> v3 auth MD5|SHA

SNMP-gebruiker <> <> v3 auth MD5/SHA <> Priv 3DES|DES56

SNMP-host <> versie 1|V2C

SNMP-groep <> v1|v2c

SNMP-communitykaart

WAARSCHUWING

-

Yang-model

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

Aanbeveling

Gebruik SNMPv3 met verificatie en codering (authPriv).

Configuratie SNMPv3 met verificatie en authPriv: Simple Network Management Protocol configureren

NTP versie 2 en 3 en MD5-verificatie

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 **<>** versie 2|3

NTP Peer **<>** versie 2/3

NTP Server Admin-Plane versie 1/2/3

NTP-interface **<>** Broadcast versie 2|3

NTP-interface **<>** multicast versie 2|3

NTP-verificatiesleutel **<>** MD5 **<>**

WAARSCHUWING

RP/0/RP0/CPU0:25 nov 16:09:15.422 UTC: ntpd[159]: %IP-IP_NTP-5-CONFIG_NOT_RECOMMENDED: NTPv2 en NTPv3 worden vanaf 25.4.1 afgeschreven. Gebruik NTPv4.

RP/0/RP0/CPU0:25 nov 16:09:15.422 UTC: ntpd[159]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Kenmerk 'NTP zonder verificatie' gebruikt of geconfigureerd. Deze functie staat bekend als onveilig, overweeg het gebruik van deze functie te staken.

Yang-model

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

Aanbeveling

Gebruik NTP versie 4 of een andere verificatie dan MD5.

NTP-configuratie: [netwerktijdprotocol configureren]

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-versie 1.0|1.1
grpc tls-chiper default|enable|disable (In TLS 1.2, onveilig wanneer onveilige coderingssuites worden gebruikt na evaluatie van de drie configuraties)

WAARSCHUWING

RP/0/RP0/CPU0:Nov 29 19:38:30.833 UTC: emsd[1122]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Kenmerk 'gRPC onveilige configuratie' gebruikt of geconfigureerd. Deze functie is verouderd omdat het bekend staat als onveilig; het zal worden verwijderd in een toekomstige release. server=DEFAULT (TLS-versie is ouder dan 1.2, onveilige coderingssuites zijn geconfigureerd)

Yang-model

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

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

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

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

Aanbeveling

Gebruik TLS 1.2 of hoger (bij voorkeur TLS 1.3) met sterke cijfers.

Configuratie: gRPC-protocol gebruiken om netwerkbewerkingen met gegevensmodellen te definiëren

Lijst met onveilige uitvoeringsopdrachten

Opdrachten kopiëren

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)
```

Kopieer <src als TFTP/FTP> <dst als TFTP/FTP>
Kopieer Running-Config?"

WAARSCHUWING

RP/0/RP0/CPU0:26 nov 15:05:57.666 UTC: filesys_cli[66940]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Functie 'copy ftp' gebruikt of geconfigureerd. Deze functie is verouderd omdat het bekend staat als onveilig; het zal worden verwijderd in een toekomstige release. Gebruik SFTP of SCP.

RP/0/RP0/CPU0:26 nov 15:09:06.181 UTC: filesys_cli[67445]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Functie 'copy TFTP' gebruikt of geconfigureerd. Deze functie is verouderd omdat het bekend staat als onveilig; het zal worden verwijderd in een toekomstige release. Gebruik SFTP of SCP.

Yang-model

-

Aanbeveling

Gebruik sFTP of SCP.

configuratie: veilige shell implementeren

Opdrachten installeren

CLI

```
install source

install add source

install replace

       "
```

WAARSCHUWING

-

Yang-model

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

Aanbeveling

Gebruik sFTP of SCP.

configuratie: veilige shell implementeren

Opdrachten voor hulpprogramma's

CLI

```
utility mv source
```

Yang Models

Er zijn te veel veranderingen in de Yang-modellen om ze allemaal hier op te sommen.

Dit is een voorbeeld voor de opmerkingen in het Yang-*modelCisco-IOS-XR-ipv4-ma-cfg*.yang voor het verwijderen van bronroutering.

```
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)";
```

Dit is een voorbeeld voor de opmerkingen in het Yang *modelCisco-IOS-XR-um-ftp-tftp-cfg*.yang voor het verwijderen van FTP en 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)";
```

Handleiding voor IOS XR-harding

De gids Cisco IOS XR Software Hardening Guide helpt netwerkbeheerders en beveiligingsprofessionals bij het beveiligen van Cisco IOS XR-gebaseerde routers om de algehele beveiligingspositie van het netwerk te verhogen.

Dit document is gestructureerd rond de drie vlakken waarmee de functies van een netwerkapparaat worden gecategoriseerd.

De drie functionele vlakken van een router zijn het managementvlak, het besturingsvlak en het gegevensvlak. Elk biedt een andere functionaliteit die moet worden beschermd.

- **Management Plane:** Het beheervlak bevat de logische groep van al het verkeer dat provisioning, onderhoud en bewakingsfuncties ondersteunt voor het Cisco IOS XR-apparaat en het netwerk. Het verkeer in deze groep omvat Secure Shell (SSH), Secure Copy Protocol (SCP), Simple Network Management Protocol (SNMP), Syslog, TACACS+, RADIUS, DNS, NetFlow en Cisco Discovery Protocol. Het vliegtuigverkeer wordt altijd beheerd met het lokale Cisco IOS XR-apparaat.
- **Controlevlak:** Het controlevlak bevat de logische groep van alle routing-, signalerings-, link-state- en andere controleprotocollen die worden gebruikt om de status van het netwerk en de interfaces ervan te maken en te onderhouden. Deze omvatten 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), en Layer 2 keepalives. Controle van vliegtuigverkeer is altijd bestemd voor het lokale Cisco IOS XR-apparaat.
- **Gegevensvlak:** Het gegevensvlak bevat de logische groep van "klant"-toepassingsverkeer dat wordt gegenereerd door hosts, clients, servers en toepassingen die afkomstig zijn van en bestemd zijn voor andere soortgelijke apparaten die door het netwerk worden ondersteund. Functies van Data Planes zijn onder andere IP-bronroutering, IP-gerichte uitzending, ICMP-omleidingen, ICMP-onbereikbare bestanden en proxy-ARP. Dataplanverkeer wordt voornamelijk doorgestuurd in het snelle pad en is nooit bestemd voor het lokale Cisco

IOS XR-apparaat.

Config Resilient Infrastructure-tester

U kunt de routerconfiguratie testen om te zien of deze veilig is of niet met deze tool die werkt voor verschillende besturingssystemen, waaronder IOS XR: Cisco Config Resilient Infrastructure Tester.

Vraag en antwoord

1. Als u een opdracht de tweede keer configureert of als u dezelfde opdracht opnieuw configureert, wordt dan hetzelfde syslog-waarschuwingsbericht opnieuw geactiveerd?

A: Nee.

2. Zullen twee configuratiecommando's voor twee verschillende functies in dezelfde commit twee syslog-waarschuwingen veroorzaken?

A: Ja.

Voorbeeld:

RP/0/RP0/CPU0:17 okt 19:01:48.806 UTC: ipv6_io[310]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Kenmerk 'IPV6 SOURCE ROUTE' gebruikt of geconfigureerd. Deze functie staat bekend als onveilig, overweeg het gebruik van deze functie te staken. Schakel IPv6-bronroutering niet in vanwege beveiligingsrisico's.

RP/0/RP0/CPU0:17 okt 19:01:48.806 UTC: ipv4_ma[254]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Kenmerk 'IPV4 SOURCE ROUTE' gebruikt of geconfigureerd. Deze functie staat bekend als onveilig, overweeg het gebruik van deze functie te staken. Schakel IPv4-bronroutering niet in vanwege beveiligingsrisico's.

3. Veroorzaakt een nieuwe opdracht voor onveilige configuratie in een nieuwe commit een nieuwe waarschuwing?

A: Ja.

4. Is er een syslog-waarschuwing wanneer de onveilige functie uit de configuratie wordt verwijderd?

A: Ja

Voorbeelden:

RP/0/RP0/CPU0:Oct 18 08:16:24.410 UTC: ssh_conf_proxy[1210]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED: Onveilige functie 'SSH host-key DSA algoritme' configuratie verwijderd.

RP/0/RP0/CPU0:Oct 22 06:37:21.960 UTC: tacacsd[1155]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED: Onveilige functie 'TACACS+ shared secret (Type 7 encoding)' configuratie verwijderd.

RP/0/RP0/CPU0:Oct 22 06:42:21.805 UTC: tacacsd[1155]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED: Onveilige functie 'TACACS+ over TCP met gedeelde geheime (standaardmodus)' configuratie verwijderd.

5. U ziet Telnet niet beschikbaar op uw router.

A: Het is mogelijk dat u IOS XR7/LNT uitvoert, waarbij Telnet alleen beschikbaar is als u de optionele Telnet RPM hebt geladen.

6. XR7/LNT heeft geen sFTP- of SCP-optie voor de opdracht "source installeren".

A: Op dit moment biedt XR7/LNT geen ondersteuning voor sFTP of SCP voor de opdracht "bron installeren".

7. Gelden de wijzigingen ook voor IOS XR eXR en IOS XR7/LNT?

A: Ja.

8. Hoe kunt u controleren of uw router IOS XR eXR of IOS XR7/LNT uitvoert

A: Gebruik "show version" en zoek naar "LNT". 8000 routers en sommige NCS540 varianten draaien op IOS XR7/LNT.

Voorbeeld:

<#root>

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

Cisco IOS XR Software, Version 25.2.2
LNT
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.