Ausfallsicherheit der Infrastruktur Cisco IOS XR

Inhalt

Einleitung

Dieses Dokument beschreibt einen Härtungsaspekt von Cisco IOS® XR: systematische Ausmusterung unsicherer Funktionen und Chiffren.

Ausfallsicherheit der Cisco IOS XR-Infrastruktur

Um den Sicherheitsstatus von Cisco Geräten zu erhöhen, nimmt Cisco Änderungen an den Standardeinstellungen vor, vernachlässigt die Sicherheitsfunktionen und entfernt sie nach und nach. Außerdem führt Cisco neue Sicherheitsfunktionen ein. Diese Änderungen dienen dazu, Ihre Netzwerkinfrastruktur zu optimieren und einen besseren Überblick über die Aktivitäten der Angreifer zu erhalten.

Weitere Informationen finden Sie auf der Seite "Trust Center": Eine ausfallsichere Infrastruktur. Er

enthält Informationen zur Infrastruktursicherung, zum Cisco IOS XR Software Hardening Guide, zum Prozess der Funktionseinschränkung sowie Details zur Funktionseinschränkung und -löschung. Die vorgeschlagenen Alternativen sind hier aufgeführt: Entfernen von Funktionen und Vorschläge für Alternativen.

Cisco IOS XR beseitigt unsichere Funktionen und Chiffren. Dies umfasst sowohl Konfigurations- als auch Ausführungsbefehle in Cisco IOS XR.

Betroffene Funktionen

- Telnet
- TFTP
- FTP
- HTTP
- SNMP v1/v2c
- SNMP v3 ohne authPriv
- IP-Quell-Route
- TCP/UDP Small Server
- TACACS+ und Radius mit Pre-Shared Keys (Typ 7) und MD5
- SSHv1
- TLS 1.0/1.1
- NTPv2/3 und MD5
- GRPC auf TLS, TLSv1.0/1.1
- Exec-Befehle mit Kopieren, Dienstprogramm und Installation über TFTP/FTP

Gruppierung

Es gibt Konfigurationsbefehle, aber auch Ausführungsbefehle (z. B. den Befehl "copy").

Die veralteten Befehle können gruppiert werden:

- SSHv1, Telnet (Server und Client), TFTP (Client), FTP
- DSA-Hostschlüssel, TACACS/RADIUS Typ 7, TLS 1.0/1.1
- Andere: Kleine TCP/UDP-Server, IP Source Routing (IPv4 und IPv6)

Phasen

Dieses Projekt folgt dem üblichen Ansatz zur Funktionseinschränkung: warnen -> einschränken -> entfernen.

- Warnungen in Cisco IOS XR, Version 25.4.1
- Restriktionsphase
- Entfernen von Funktionen

Warnphase

Wie lauten die Warnungen?

1. Die CLI-Hilfefunktion (Command Line Interface)
2. Eine Syslog-Warnung

3. Eine Beschreibung im Yang-Modul

Bei konfigurierten unsicheren Optionen werden Warnungen ausgegeben. Dies sind Syslog-Meldungen mit **einer Häufigkeit von 30 Tagen**.

Wenn eine nicht sichere Funktion verwendet wird, wird diese Protokollwarnung (Stufe 4 oder Warnung) ausgegeben:

*%**INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN**: Die Funktion '<Funktionsname>' wurde verwendet oder konfiguriert. Diese Funktion ist als unsicher bekannt. Sie können die Verwendung dieser Funktion beenden. <Empfehlung>*

Es wird empfohlen, anstelle der unsicheren Option zu verwenden.

Beispiel für eine FTP-Warnung:

%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Funktion "FTP" wird verwendet oder konfiguriert. Diese Funktion ist als unsicher bekannt. Sie können die Verwendung dieser Funktion beenden. Empfehlung von SFTP.

Beachten Sie die verwendeten oder konfigurierten Wörter. Utilized bezieht sich auf einen Ausführungsbefehl und configured bezieht sich auf einen Konfigurationsbefehl.

Eine Warnmeldung kann ausgegeben werden, wenn die Option "Unsicher" entfernt wird (Stufe 6 oder informativ). Beispiel:

RP/0/RP0/CPU0:Okt 22 06:43:43.967 UTC: tacacsd[1155]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED : Die unsichere Funktion "TACACS+ over TCP with shared secret (Standardmodus)" wurde entfernt.

Liste veralteter und unsicherer Optionen

Dies ist die Liste der unsicheren Optionen, die bei Cisco IOS XR-Versionen der Warnphase eine Warnung auslösen.

Die Liste zeigt die unsichere Option, die Konfigurations- oder Ausführungsbefehle, die Warnmeldung und das zugehörige Yang-Modell.

IP Source Routing (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-Quellroute

IPv6-Quellroute

IPv4-Quellroute

Warnung

RP/0/RP0/CPU0:Okt 17 19:01:48.806 UTC: ipv4_ma[254]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Die Funktion "IPV4 SOURCE ROUTE" wird verwendet oder konfiguriert. Diese Funktion ist als unsicher bekannt. Sie können die Verwendung dieser Funktion beenden. Aktivieren Sie IPv4 Source Routing aufgrund von Sicherheitsrisiken nicht.

RP/0/RP0/CPU0:Okt 17 19:01:48.806 UTC: ipv6_io[310]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Die Funktion "IPV6 SOURCE ROUTE" wird verwendet oder konfiguriert. Diese Funktion ist als unsicher bekannt. Sie können die Verwendung dieser Funktion beenden. Aktivieren Sie IPv6 Source Routing aufgrund von Sicherheitsrisiken nicht.

Yang-Modell

Cisco-IOS-XR-ipv4-ma-cfg

Cisco IOS-XR-IPv6-io-cfg

Cisco-IOS-XR-um-ipv4-cfg

Cisco-IOS-XR-um-IPv6-cfg

Empfehlung

Entfernen Sie die unsichere Option.

Es gibt keine genaue Alternative. Kunden, die den Datenverkehr über ein Netzwerk anhand der Quelladresse steuern möchten, können dazu richtlinienbasiertes Routing oder andere vom Administrator gesteuerte Source-Routing-Mechanismen verwenden, die die Routing-Entscheidung nicht dem Endbenutzer überlassen.

SSHv1

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

Warnung

RP/0/RP0/CPU0:19. November 15:20:42,814 UTC: ssh_conf_proxy[1210]: %SECURITY-SSHD_CONF_PRX-4-WARNUNG_ALLGEMEIN: Backup-Server, Netconf-Port-Konfigurationen, SSH v1, SSH-Port werden von dieser Plattform nicht unterstützt. Version wird nicht übernommen.

Yang-Modell

Cisco-IOS-XR-um-ssh-cfg

Empfehlung

Verwenden Sie SSH v2.

Konfiguration von SSHv2: Implementieren von Secure Shell

TACACS+ und Radius mit vorinstallierten Schlüsseln (Typ 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-Serverschlüssel 7 135445410615102B28252B203E270A

tacacs-server host 10,1.1,1 port 49

Schlüssel 7 1513090F007B7977

radius-server host 10,0.0,1 auth-port 9999 acct-port 8888

Schlüssel 7 1513090F007B7977

aaa server radius dynamic-author

client 10.10.10.2 vrf default

Serverschlüssel 7 05080F1C2243

radius-server key 7 130415110F

aaa Gruppenserver Radius RAD

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

Schlüssel 7 1304464058

Warnung

RP/0/RP0/CPU0:Okt 18 18:00:42.505 UTC: tacacsd[1155]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Die Funktion "TACACS+ shared secret (Codierung vom Typ 7)" wird verwendet oder konfiguriert. Diese Funktion ist als unsicher bekannt. Sie können die Verwendung dieser Funktion beenden. Verwenden Sie stattdessen die Typ-6-Verschlüsselung (AES-basiert).

RP/0/RP0/CPU0:Okt 18 18:00:42.505 UTC: tacacsd[1155]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Die Funktion "TACACS+ over TCP with shared secret (Standardmodus)" wird verwendet oder konfiguriert. Diese Funktion ist als unsicher bekannt. Sie können die Verwendung dieser Funktion beenden. Stärkere Sicherheit mit TACACS+ über TLS (Secure TACACS+)

RP/0/RP0/CPU0:Okt 18 18:18:19.460 UTC: radiusd[1149]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Die Funktion "RADIUS shared secret (Codierung vom Typ 7)" wird verwendet oder konfiguriert. Diese Funktion ist als unsicher bekannt. Sie können die Verwendung dieser Funktion beenden. Verwenden Sie stattdessen die Typ-6-Verschlüsselung (AES-basiert).

RP/0/RP0/CPU0:Okt 18 18:18:19.460 UTC: radiusd[1149]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Die Funktion "RADIUS over UDP with shared secret (Standardmodus)" wird verwendet oder konfiguriert. Diese Funktion ist als unsicher bekannt. Sie können die Verwendung dieser Funktion beenden. Verwenden Sie RADIUS over TLS (RadSec) oder DTLS, um eine höhere Sicherheit zu gewährleisten.

Yang-Modell

-

Empfehlung

Verwenden Sie TACACS+ oder Radius über TLS 1.3 oder DTLS. Geben Sie als Anmeldeinformationen Typ 6 ein.

Konfiguration von TACACS+ oder Radius über TLS 1.3 oder DTLS: Konfigurieren von AAA-Services

TLS 1.0/1.1, veraltete schwache Chiffren

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 Servername <> max-version tls1.0|tls1.1

Warnung

-

Yang-Modell

Cisco-IOS-XR-um-logging-cfg

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

Empfehlung

Verwenden Sie TLS1.2 oder TLS1.3.

Sichere Protokollierung der Konfiguration: Implementieren der sicheren Protokollierung

Telnet (Server und 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

Warnung

RP/0/RP0/CPU0:27. Juni 10:59:52.226 UTC: cinetd[145]: %IP-CINETD-4-TELNET_WARNUNG: Die Telnet-Unterstützung ist seit Version 25.4.1 veraltet. Verwenden Sie stattdessen SSH.

Yang-Modell

Cisco-IOS-XR-ipv4-telnet-cfg

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

Cisco-IOS-XR-um-telnet-cfg

Empfehlung

Verwenden Sie SSHv2.

Konfiguration von SSHv2: Implementieren von Secure Shell

TFTP (Server und 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

Warnung

RP/0/RP0/CPU0:Okt 17 19:03:29.475 UTC: tftp_fs[414]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Funktion "TFTP-Client" wird verwendet oder konfiguriert. Diese Funktion ist als unsicher bekannt. Sie können die Verwendung dieser Funktion beenden. Verwenden Sie stattdessen SFTP.

Yang-Modell

-

Empfehlung

Verwenden Sie sFTP oder HTTPS.

Configuration sFTP: Implementing Secure Shell

Kleine TCP/UDP-Server

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

Warnung

-

Yang-Modell

Cisco-IOS-XR-ip-tcp-cfg

Cisco-IOS-XR-ip-udp-cfg

Empfehlung

Deaktivieren Sie kleine TCP/UDP-Server.

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

Warnung

RP/0/RP0/CPU0:Okt 16 21:42:42.897 UTC: ftp_fs[1190]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Die Funktion "FTP-Client" wird verwendet oder konfiguriert. Diese Funktion ist als unsicher bekannt. Sie können die Verwendung dieser Funktion beenden. Verwenden Sie stattdessen SFTP.

Yang-Modell

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

Empfehlung

Verwenden Sie sFTP oder HTTPS.

Configuration sFTP: Implementing 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 benutzer <> <> v1 | v2c

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

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

snmp-server host <> version 1|v2c

snmp-server group <> v1|v2c

snmp-server community-map

SNMP-Community

snmp benutzer <> <> v1|v2c

snmp benutzer <> <> v3 auth md5|sha

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

snmp host <> version 1|v2c

snmp group <> v1|v2c

snmp community-map

Warnung

-

Yang-Modell

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

Empfehlung

Verwenden Sie SNMPv3 mit Authentifizierung und Verschlüsselung (authPriv).

Konfiguration von SNMPv3 mit Authentifizierung und AuthentifizierungPriv: Konfigurieren des Simple Network Management Protocol

NTP-Authentifizierung Version 2 und 3 und 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 **<>** **<>**

Warnung

RP/0/RP0/CPU0:25. November 16:09:15.422 UTC: ntpd[159]: %IP-IP_NTP-5-CONFIG_NOT_EMPFOHLEN : NTPv2 und NTPv3 sind seit 25.4.1 veraltet. Verwenden Sie NTPv4.

RP/0/RP0/CPU0:25. November 16:09:15.422 UTC: ntpd[159]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Die Funktion "NTP ohne Authentifizierung" wird verwendet oder konfiguriert. Diese Funktion ist als unsicher bekannt. Sie können die Verwendung dieser Funktion beenden.

Yang-Modell

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

Empfehlung

Verwenden Sie NTP-Version 4 oder eine andere Authentifizierung als MD5.

Konfiguration NTP: Konfigurieren des Network Time Protocol

GRPC

CLI

<#root>

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

grpc ?

```
  aaa                          AAA authorization and authentication for gRPC
  address-family               DEPRECATED. Removing in 26.3.1: Address family identifier type
  apply-group                  Apply configuration from a group
  certificate                  DEPRECATED. Removing in 26.3.1: gRPC server certificate
  certificate-authentication   DEPRECATED. Removing in 26.3.1: Enables Certificate based Authentication
  certificate-id               DEPRECATED. Removing in 26.3.1: Active Certificate
  default-server-disable       Configuration to disable the default gRPC server
  dscp                         DEPRECATED. Removing in 26.3.1: QoS marking DSCP to be set on transmitted
  exclude-group                Exclude apply-group configuration from a group
  gnmi                         gNMI service configuration
  gnpsi                        gnpsi configuration
  gnsi                         gNSI
  gribi                        gRIBI service configuration
  keepalive                    DEPRECATED. Removing in 26.3.1: Server keepalive time and timeout
  listen-addresses             DEPRECATED. Removing in 26.3.1: gRPC server listening addresses
  local-connection             DEPRECATED. Removing in 26.3.1: Enable gRPC server over Unix socket
  max-concurrent-streams       gRPC server maximum concurrent streams per connection
  max-request-per-user         Maximum concurrent requests per user
  max-request-total            Maximum concurrent requests in total
  max-streams                  Maximum number of streaming gRPCs (Default: 32)
  max-streams-per-user         Maximum number of streaming gRPCs per user (Default: 32)
  memory                       EMSd-Go soft memory limit in MB
  min-keepalive-interval       DEPRECATED. Removing in 26.3.1: Minimum client keepalive interval
  name                         DEPRECATED. Removing in 26.3.1: gRPC server name
  no-tls                       DEPRECATED. Removing in 26.3.1: No TLS
  p4rt                         p4 runtime configuration
  port                         DEPRECATED. Removing in 26.3.1: Server listening port
  remote-connection            DEPRECATED. Removing in 26.3.1: Configuration to toggle TCP support on th
  segment-routing              gRPC segment-routing configuration
  server                       gRPC server configuration
  service-layer                grpc service layer configuration
  tls-cipher                   DEPRECATED. Removing in 26.3.1: gRPC TLS 1.0-1.2 cipher suites
  tls-max-version              DEPRECATED. Removing in 26.3.1: gRPC maximum TLS version
  tls-min-version              DEPRECATED. Removing in 26.3.1: gRPC minimum TLS version
  tls-mutual                   DEPRECATED. Removing in 26.3.1: Mutual Authentication
  tls-trustpoint               DEPRECATED. Removing in 26.3.1: Configure trustpoint
```

```
  tlsV1-disable               Disable support for TLS version 1.0
                              tlsv1-disable CLI is deprecated.
                              Use tls-min-version CLI to set minimum TLS version.
  ttl                         DEPRECATED. Removing in 26.3.1: gRPC packets TTL value
  tunnel                      DEPRECATED. Removing in 26.3.1: grpc tunnel service
  vrf                         DEPRECATED. Removing in 26.3.1: Server vrf
  <cr>
```

grpc no-tls
grpc tls-max|min-Version 1.0|1.1
grpc tls-cihper default|enable|disable (Unsicher in TLS 1.2, wenn nach Auswertung der drei Konfigurationen unsichere Chiffriersuiten verwendet werden)

Warnung

RP/0/RP0/CPU0:29. November 19:38:30,833 UTC: emsd[1122]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Die Funktion "gRPC insecure configuration" wird verwendet oder konfiguriert. Diese Funktion ist veraltet, da sie als unsicher gilt. wird es in einer zukünftigen Version entfernt. server=DEFAULT (TLS-Version ist älter als 1.2, unsichere Verschlüsselungssuiten sind konfiguriert)

Yang-Modell

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

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

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

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

Empfehlung

Verwenden Sie TLS 1.2 oder höher (vorzugsweise TLS 1.3) mit starken Chiffren.

Konfiguration: Verwenden des gRPC-Protokolls zum Definieren von Netzwerkoperationen mit Datenmodellen

Liste unsicherer Ausführungsbefehle

Befehle kopieren

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 ?"

Warnung

RP/0/RP0/CPU0:26. November 15:05:57,666 UTC: filesys_cli[66940]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Die Funktion "copy ftp" wird verwendet oder konfiguriert. Diese Funktion ist veraltet, da sie als unsicher gilt. wird es in einer zukünftigen Version entfernt. Verwenden Sie stattdessen SFTP oder SCP.

RP/0/RP0/CPU0:26. November 15:09:06.181 UTC: filesys_cli[67445]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Die Funktion "copy tftp" wird verwendet oder konfiguriert. Diese Funktion ist veraltet, da sie als unsicher gilt. wird es in einer zukünftigen Version entfernt. Verwenden Sie stattdessen SFTP oder SCP.

Yang-Modell

-

Empfehlung

sFTP oder SCP verwenden.

Konfiguration: Implementieren von Secure Shell

Installationsbefehle

CLI

```
install source

install add source

install replace

       "
```

Warnung

-

Yang-Modell

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

Empfehlung

sFTP oder SCP verwenden.

Konfiguration: Implementieren von Secure Shell

Dienstprogrammbefehle

CLI

```
utility mv source
```

Yang Models

Es gibt zu viele Änderungen in den Yang-Modellen, um sie alle hier aufzulisten.

Dies ist ein Beispiel für die Kommentare im Yang-*ModellCisco-IOS-XR-ipv4-ma-cfg*.yang zum Entfernen von Source-Routing.

```
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)";
```

Dies ist ein Beispiel für die Kommentare im Yang-*ModellCisco-IOS-XR-um-ftp-tftp-cfg*.yang zum Entfernen von FTP und 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)";
```

IOS XR-Härtungsleitfaden

Der Leitfaden Cisco IOS XR Software Hardening Guide unterstützt Netzwerkadministratoren und Sicherheitsexperten bei der Sicherung von Cisco IOS XR-basierten Routern, um den allgemeinen Sicherheitsstatus des Netzwerks zu erhöhen.

Dieses Dokument ist um die drei Ebenen herum strukturiert, nach denen die Funktionen eines Netzwerkgeräts kategorisiert sind.

Die drei Funktionsebenen eines Routers sind die Management-, die Kontroll- und die Datenebene. Jede bietet eine andere Funktionalität, die geschützt werden muss.

- **Verwaltungsebene:** Die Verwaltungsebene enthält die logische Gruppe des gesamten Datenverkehrs, die Bereitstellungs-, Wartungs- und Überwachungsfunktionen für das Cisco IOS XR-Gerät und das Netzwerk unterstützt. Der Datenverkehr in dieser Gruppe umfasst Secure Shell (SSH), Secure Copy Protocol (SCP), Simple Network Management Protocol (SNMP), Syslog, TACACS+, RADIUS, DNS, NetFlow und Cisco Discovery Protocol. Der Datenverkehr auf Verwaltungsebene ist immer für das lokale Cisco IOS XR-Gerät bestimmt.
- **Kontrollebene:** Die Kontrollebene enthält die logische Gruppe aller Routing-, Signalisierungs-, Link-State- und anderer Kontrollprotokolle,

die verwendet werden, um den Status des Netzwerks und seiner Schnittstellen zu erstellen und aufrechtzuerhalten. Dazu gehören 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) und Layer-2-Keepalive. Der Datenverkehr auf der Kontrollebene ist immer für das lokale Cisco IOS XR-Gerät bestimmt.

- **Datenebene:** Die Datenebene enthält die logische Gruppe von Anwendungsdatenverkehr des Kunden, der von Hosts, Clients, Servern und Anwendungen generiert wird, die von anderen ähnlichen Geräten stammen und für diese bestimmt sind, die vom Netzwerk unterstützt werden. Zu den Funktionen der Datenebene gehören IP Source Routing, IP Directed Broadcast, ICMP Redirects, ICMP Unreachables und Proxy ARP. Datenverkehr auf Datenebene wird hauptsächlich über den schnellen Pfad weitergeleitet und niemals an das lokale Cisco IOS XR-Gerät weitergeleitet.

Test der ausfallsicheren Infrastruktur konfigurieren

Sie können die Router-Konfiguration testen, um festzustellen, ob sie sicher ist oder nicht. Verwenden Sie dazu dieses Tool, das für mehrere Betriebssysteme verwendet werden kann, z. B. IOS XR: Cisco Config Resilient Infrastructure Tester.

Fragen und Antworten

1. Wenn Sie beim zweiten Mal einen Befehl konfigurieren oder den gleichen Befehl erneut konfigurieren, löst dies dann erneut die gleiche Syslog-Warnmeldung aus?

A : Nein.

2. Werden zwei Konfigurationsbefehle für zwei verschiedene Funktionen im gleichen Commit zwei Syslog-Warnungen verursachen?

A : Ja.

Beispiel:

RP/0/RP0/CPU0:Okt 17 19:01:48.806 UTC: ipv6_io[310]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Die Funktion "IPV6 SOURCE ROUTE" wird verwendet oder konfiguriert. Diese Funktion ist als unsicher bekannt. Sie können die Verwendung dieser Funktion beenden. Aktivieren Sie IPv6 Source Routing aufgrund von Sicherheitsrisiken nicht.

RP/0/RP0/CPU0:Okt 17 19:01:48.806 UTC: ipv4_ma[254]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: Die Funktion "IPV4 SOURCE ROUTE" wird verwendet oder konfiguriert. Diese Funktion ist als unsicher bekannt. Sie können die Verwendung dieser Funktion beenden. Aktivieren Sie IPv4 Source Routing aufgrund von Sicherheitsrisiken nicht.

3. Wird ein neuer unsicherer Konfigurationsbefehl in einem neuen Commit eine neue Warnung auslösen?

A : Ja.

4. Gibt es eine Syslog-Warnung, wenn die unsichere Funktion aus der Konfiguration entfernt wird?

A : Ja

Beispiele:

RP/0/RP0/CPU0:Okt 18 08:16:24.410 UTC: ssh_conf_proxy[1210]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED : Die unsichere Konfiguration der SSH-Hostschlüssel-DSA-Algorithmus-Funktion wurde entfernt.

RP/0/RP0/CPU0:Okt 22 06:37:21.960 UTC: tacacsd[1155]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED : Die unsichere Konfiguration der Funktion 'TACACS+ shared secret (Codierung vom Typ 7)' wurde entfernt.

RP/0/RP0/CPU0:Okt 22 06:42:21.805 UTC: tacacsd[1155]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED : Die unsichere Funktion "TACACS+ over TCP with shared secret (Standardmodus)" wurde entfernt.

5. Auf Ihrem Router ist Telnet nicht verfügbar.

A : Es ist möglich, dass Sie IOS XR XR7/LNT ausführen, bei dem Telnet nur verfügbar ist, wenn Sie die optionale Telnet-RPM geladen haben.

6. Es wird nicht angezeigt, dass XR7/LNT die Option sFTP oder SCP für den Befehl "install source" aufweist.

A : Zurzeit unterstützt XR7/LNT weder sFTP noch SCP für den Befehl "install source".

7. Gelten die Änderungen gleichermaßen für IOS XR eXR und IOS XR XR7/LNT?

A : Ja.

8. Wie können Sie überprüfen, ob auf Ihrem Router IOS XR eXR oder IOS XR XR7/LNT ausgeführt wird?

A : Verwenden Sie "Version anzeigen" und suchen Sie nach "LNT". Auf 8000-Routern und einigen NCS540-Varianten wird IOS XR7/LNT ausgeführt.

Beispiel:

<#root>

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

Cisco IOS XR Software, Version 25.2.2
LNT
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.