

基礎架構可復原性Cisco IOS XR

目錄

[簡介](#)

[Cisco IOS XR基礎架構彈性](#)

[受影響的功能](#)

[分組](#)

[階段](#)

[警告階段](#)

[已棄用的不安全選項清單](#)

[IP來源路由\(RFC 791\)](#)

[SSH v1](#)

[具有預共用金鑰的TACACS+和Radius \(型別7 \)](#)

[TLS 1.0/1.1, 棄用弱密碼](#)

[Telnet \(伺服器 and 客戶端 \)](#)

[TFTP \(伺服器 and 使用者端 \)](#)

[TCP/UDP小型伺服器](#)

[FTP](#)

[SNMP v1/2c](#)

[NTP第2版和第3版以及MD5身份驗證](#)

[GRPC](#)

[不安全的執行命令清單](#)

[複製命令](#)

[安裝命令](#)

[實用程式命令](#)

[楊模型](#)

[IOS XR強化指南](#)

[Config Resilient Infrastructure Tester](#)

[版本和一般資料](#)

簡介

本檔案介紹Cisco IOS® XR的一個強化方面:系統地逐步消除不安全的功能和密碼。

Cisco IOS XR基礎架構彈性

為了提高思科裝置的安全狀態，思科正在對預設設定進行更改，淘汰並最終刪除不安全的功能，並引入新的安全功能。這些更改旨在增強您的網路基礎設施，並更好地檢視威脅實施者的活動。

請關注此信任中心頁面：可恢復的[基礎設施](#)。其中提到基礎架構強化、Cisco IOS XR軟體強化指南、功能棄用過程以及功能[棄用和刪除詳細資訊](#)。此處提到了建議的替代方案：[功能刪除和建議的替代方案](#)。

Cisco IOS XR正在逐步淘汰不安全的功能和密碼。這包括Cisco IOS XR中的配置命令和執行命令。

受影響的功能

- Telnet
- TFTP
- FTP
- HTTP
- SNMP v1/v2c
- 不帶authPriv的SNMP v3
- IP源路由
- TCP/UDP小型伺服器
- 具有預共用金鑰 (型別7) 和MD5的TACACS+和Radius
- SSH v1
- TLS 1.0/1.1
- NTPv2/3和MD5
- GRPC , 無TLS , TLSv1.0/1.1
- 使用copy、utility和install with TFTP/FTP執行命令

分組

有配置命令，但也有執行命令 (例如「copy」命令) 。

已棄用的命令可以分組：

- SSHv1、Telnet (伺服器和客戶端) 、TFTP (客戶端) 、FTP
- DSA主機金鑰，TACACS/RADIUS型別7,TLS 1.0/1.1
- 其他:TCP/UDP小型伺服器、IP源路由 (IPv4和IPv6)

階段

此專案遵循通常的特徵棄用方法：警告 —>限制 —>刪除。

- Cisco IOS XR 25.4.1版中的警告。
- 限制階段
- 功能刪除

警告階段

警告是什麼？

1. CLI (命令列介面) 幫助功能
2. 系統日誌警告
3. Yang模組中的描述警告

對配置的不安全選項發出警告。這些是頻率30天的系統日誌消息。

使用任何不安全功能時，會發出此日誌警告 (級別4或警告) ：

%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN:已使用或配置功能「<feature-name>」。此功能已知不安全，請考慮停

止使用此功能。<建議>

建議使用什麼來代替不安全選項。

FTP警告示例：

`%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN`:已使用或配置功能「*FTP*」。此功能已知不安全，請考慮停止使用此功能。建議使用*SFTP*。

請注意所用或配置的字詞。Used指執行命令，configured指配置命令。

如果刪除了不安全的選項（級別6或資訊性），可以列印一條警告消息。範例：

`RP/0/RP0/CPU0:Oct 22 06:43:43.967 UTC:tacacsd[115]:%INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED`:已刪除不安全功能「*TACACS+ over TCP with shared secret(default mode)*」(使用共用金鑰 (預設模式) 的*TACACS+*)配置。

已棄用的不安全選項清單

這是在Cisco IOS XR版本中的警告階段觸發警告的不安全選項清單。

該清單顯示了不安全選項、配置或執行命令、警告消息以及相關的Yang模型。

IP來源路由(RFC 791)

CLI

<#root>

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

ip ?

source-route Process packets with source routing header options (This is deprecated since

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

ipv4 ?

source-route Process packets with source routing header options (This is deprecated since

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

ipv6 ?

source-route Process packets with source routing header options (This is deprecated since

ip source route

ipv6 source-route

ipv4 source-route

警告

RP/0/RP0/CPU0:Oct 17 19:01:48.806 UTC:ipv4_ma[254]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN:已使用或配置功能「IPV4源路由」。此功能已知不安全，請考慮停止使用此功能。由於安全風險，請勿啟用IPv4源路由。

RP/0/RP0/CPU0:Oct 17 19:01:48.806 UTC:ipv6_io[310]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN:已使用或配置功能「IPV6源路由」。此功能已知不安全，請考慮停止使用此功能。由於存在安全風險，請不要啟用IPv6源路由。

楊氏模型

Cisco-IOS-XR-ipv4-ma-cfg

Cisco-IOS-XR-ipv6-io-cfg

Cisco-IOS-XR-um-ipv4-cfg

Cisco-IOS-XR-um-ipv6-cfg

建議

刪除不安全選項。

不存在確切的替代方案。希望根據源地址控制網路流量的客戶可以使用基於策略的路由或其他管理員控制的源路由機制（不將路由決策留給終端使用者）進行控制。

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 25.3.1.

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

ssh server ?

v1

Cisco sshd protocol version 1. This is deprecated in 25.3.1.

ssh客戶端v1

ssh伺服器v1

警告

RP/0/RP0/CPU0:11月19日15:20:42.814 UTC:ssh_conf_proxy[1210]:%SECURITY-SSHD_CONF_PRX-4-WARNING_GENERAL :備份伺服器、netconf埠配置、ssh v1、ssh埠在此平台中不受支援，且版本不會生效

楊氏模型

Cisco-IOS-XR-um-ssh-cfg

建議

使用SSH v2。

配置SSHv2：[實施安全外殼](#)

具有預共用金鑰的TACACS+和Radius（型別7）

CLI

<#root>

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

tacacs-server host 10.0.0.1

RP/0/RP0/CPU0:Router(config-tacacs-host)#

key ?

clear Config deprecated from 7.4.1. Use '0' instead.
encrypted Config deprecated from 7.4.1. Use '7' instead.

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

tacacs-server key ?

clear Config deprecated from 7.4.1. Use '0' instead.
encrypted Config deprecated from 7.4.1. Use '7' instead.

tacacs-server key 7 135445410615102B28252B203E270A

tacacs伺服器主機10.1.1.1埠49

金鑰7 1513090F007B7977

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

金鑰7 1513090F007B7977

```
aaa server radius dynamic-author
```

客戶端10.10.10.2 vrf預設值

```
server-key 7 05080F1C2243
```

```
radius伺服器金鑰7 130415110F
```

```
aaa群組伺服器radius RAD
```

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

```
金鑰7 1304464058
```

警告

RP/0/RP0/CPU0:Oct 18 18:00:42.505 UTC:tacacsd[115]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN:已使用或配置功能「TACACS+共用金鑰 (型別7編碼)」。此功能已知不安全，請考慮停止使用此功能。改用型別6 (基於AES) 加密。

RP/0/RP0/CPU0:Oct 18 18:00:42.505 UTC:tacacsd[115]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN:已使用或配置功能「TACACS+ over TCP with shared secret(default mode)(使用共用金鑰的TACACS+ (預設模式))」。此功能已知不安全，請考慮停止使用此功能。使用TACACS+ over TLS (安全TACACS+) 增強安全性。

RP/0/RP0/CPU0:10月18日18:18:19.460 UTC:radiusd[1149]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN:已使用或配置功能「RADIUS共用金鑰 (型別7編碼)」。此功能已知不安全，請考慮停止使用此功能。改用型別6 (基於AES) 加密。

RP/0/RP0/CPU0:10月18日18:18:19.460 UTC:radiusd[1149]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN:已使用或配置功能「RADIUS over UDP with shared secret(default mode)」。此功能已知不安全，請考慮停止使用此功能。使用RADIUS over TLS(RadSec)或DTLS實現更強的安全性。

楊氏模型

-

建議

使用TACACS+或TLS 1.3或DTLS上的Radius。使用型別6作為憑證。

配置通過TLS 1.3或DTLS的TACACS+或Radius：[配置AAA服務](#)

TLS 1.0/1.1，棄用弱密碼

CLI

<#root>

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

```
http client ssl version ?
```

```
tls1.0 Force TLSv1.0 to be used for HTTPS requests, TLSv1.0 is deprecated from 25.3.1
tls1.1 Force TLSv1.1 to be used for HTTPS requests, TLSv1.1 is deprecated from 25.3.1
```

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

logging tls-server server-name min-version ?

```
tls1.0 Set TLSv1.0 to be used as min version for syslog, TLSv1.0 is deprecated from 25.3.1
tls1.1 Set TLSv1.1 to be used as min version for syslog, TLSv1.1 is deprecated from 25.3.1
```

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

logging tls-server server-name max-version ?

```
tls1.0 Set TLSv1.0 to be used as max version for syslog, TLSv1.0 is deprecated from 25.3.1
tls1.1 Set TLSv1.1 to be used as max version for syslog, TLSv1.1 is deprecated from 25.3.1
```

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

警告

-

楊氏模型

Cisco-IOS-XR-um-logging-cfg

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

建議

使用TLS1.2或TLS1.3。

配置安全記錄：[實施安全記錄](#)

Telnet (伺服器 and 客戶端)

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 recommended instead.)
server Telnet server configuration commands. (Telnet is deprecated since 25.4.1. SSH is recommended instead.)

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

telnet ipv6 ?

client Telnet client configuration commands. (Telnet is deprecated since 25.4.1. SSH is recommended instead.)
server Telnet server configuration commands. (Telnet is deprecated since 25.4.1. SSH is recommended instead.)

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 recommended instead.)
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 recommended instead.)
vrf	vrf table for the route lookup. (Telnet is deprecated since 25.4.1. SSH is recommended instead.)

telnet

telnet ipv4

telnet ipv6

telnet vrf

警告

RP/0/RP0/CPU0:6月27日10:59:52.226 UTC:cinetd[145]:%IP-CINETD-4-TELNET_WARNING:從25.4.1開始，不再支援Telnet。請改用SSH。

楊氏模型

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

Cisco-IOS-XR-um-telnet-cfg

建議

使用SSHv2。

配置SSHv2：[實施安全外殼](#)

TFTP（伺服器和使用端）

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客戶端

警告

RP/0/RP0/CPU0:Oct17 19:03:29.475 UTC:tftp_fs[414]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN:已使用或配置功能「TFTP客戶端」。此功能已知不安全，請考慮停止使用此功能。請改用SFTP。

楊氏模型

-

建議

使用sFTP或HTTPS。

配置sFTP：[實施安全外殼](#)

TCP/UDP小型伺服器

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)

服務ipv4

服務ipv6

警告

-

楊氏模型

Cisco-IOS-XR-ip-tcp-cfg

Cisco-IOS-XR-ip-udp-cfg

建議

禁用TCP/UDP小型伺服器。

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 instead

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

ip ftp ?

client FTP client config commands.This is deprecated since 25.4.1.SFTP is recommended instead

ip ftp

ftp

警告

RP/0/RP0/CPU0:Oct16 21:42:42.897 UTC:ftp_fs[1190]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN:已使用或配置功能「FTP客戶端」。此功能已知不安全，請考慮停止使用此功能。請改用SFTP。

楊氏模型

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

建議

使用sFTP或HTTPS。

配置sFTP：[實施安全外殼](#)

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 deprecated since 25.4.1)

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

snmp-server ?

community	Enable SNMP; set community string and access privileges. (This is deprecated since 25.4.1)
-----------	--

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 deprecated since 25.4.1)
- 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 deprecated since 25.4.1)

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

snmp user user test ?

- remote Specify a remote SNMP entity to which the user belongs
- v1 user using the v1 security model (This is deprecated since 25.4.1)
- v2c user using the v2c security model (This is deprecated since 25.4.1)

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

snmp-server user user1 group1 v3 auth ?

- md5 Use HMAC MD5 algorithm for authentication (This is deprecated since 25.4.1)
- sha Use HMAC SHA algorithm for authentication (This is deprecated since 25.4.1)

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

snmp user user1 group1 v3 auth ?

md5 Use HMAC MD5 algorithm for authentication (This is deprecated since 25.4.1)
sha Use HMAC SHA algorithm for authentication (This is deprecated since 25.4.1)

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

snmp user user1 group1 v3 auth md5 test priv ?

3des Use 168 bit 3DES algorithm for encryption (This is deprecated since 25.4.1)
des56 Use 56 bit DES algorithm for encryption (This is deprecated since 25.4.1)

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

snmp host 10.1.1.1 version ?

1 Use 1 for SNMPv1. (This is deprecated since 25.4.1)
2c Use 2c for SNMPv2c. (This is deprecated since 25.4.1)

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

snmp-server host 10.1.1.1 version ?

1 Use 1 for SNMPv1. (This is deprecated since 25.4.1)
2c Use 2c for SNMPv2c. (This is deprecated since 25.4.1)

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

snmp ?

community-map Community Mapping as per RFC-2576. (This is deprecated since 25.4.1)

snmp-server community

snmp-server user <> <> v1 | v2c

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

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

snmp-server host <>版本1|v2c

snmp-server group <> v1|v2c

snmp-server community-map

snmp社群

snmp user <> <> v1|v2c

snmp user <> <> v3 auth md5|sha

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

snmp host <>版本1|v2c

snmp group <> v1|v2c

snmp community-map

警告

-

楊氏模型

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

建議

將SNMPv3與驗證和加密(authPriv)一起使用。

配置帶有身份驗證和authPriv的SNMPv3：配置[簡單網路管理協定](#)

NTP第2版和第3版以及MD5身份驗證

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 <>版本2|3
```

```
ntp peer <>版本2/3
```

```
ntp server admin-plane version 1/2/3
```

```
ntp interface <>廣播版本2|3
```

```
ntp interface <>組播版本2|3
```

```
ntp authentication-key <> md5 <> <>
```

警告

RP/0/RP0/CPU0:11月25日16:09:15.422 UTC:ntpd[159]:%IP-IP_NTP-5-CONFIG_NOT_RECOMMENDED:NTPv2和NTPv3自25.4.1起被棄用。請使用NTPv4。

RP/0/RP0/CPU0:11月25日16:09:15.422 UTC:ntpd[159]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN :已使用或配置功能「NTP with no authentication」。此功能已知不安全，請考慮停止使用此功能。

楊氏模型

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

建議

使用NTP第4版或MD5以外的身份驗證。

配置NTP：配置[網路時間協定](#)

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 the
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 (在TLS 1.2中，在評估三個配置後使用不安全的密碼套件時是不安全的)

警告

RP/0/RP0/CPU0:11月29日19:38:30.833 UTC:emsd[112]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN :已使用或配置功能「gRPC不安全配置」。此功能已棄用，因為它已知不安全；在以後的版本中將會將其刪除。server=DEFAULT (TLS版本早於1.2，已配置不安全的密碼套件)

楊氏模型

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

建議

使用具有強密碼的TLS 1.2或更高版本（最好是TLS 1.3）。

配置：使用[gRPC協定定義資料模型的網路操作](#)

不安全的執行命令清單

複製命令

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 ?"

警告

RP/0/RP0/CPU0:11月26日15:05:57.666 UTC:filesys_cli[66940]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN:已使用或配置功能「copy ftp」。此功能已棄用，因為它已知不安全；在以後的版本中將會將其刪除。請改用SFTP或SCP。

RP/0/RP0/CPU0:11月26日15:09:06.181 UTC:filesys_cli[67445]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN:已使用或配置功能「copy tftp」。此功能已棄用，因為它已知不安全；在以後的版本中將會將其刪除。請改用SFTP或SCP。

楊氏模型

-

建議

使用sFTP或SCP。

配置：實[施安全外殼](#)

安裝命令

CLI

install source

install add source

install replace

"

警告

-

楊氏模型

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

建議

使用sFTP或SCP。

配置：實[施安全外殼](#)

實用程式命令

CLI

utility mv source

楊模型

Yang模型中有太多更改，無法全部列出。

以下是Yang型號*Cisco-IOS-XR-ipv4-ma-cfg.yang*中用於刪除源路由的註釋的示例。

```
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)";
```

以下是Yang型號*Cisco-IOS-XR-um-ftp-tftp-cfg.yang*中用於刪除FTP和TFTP的註釋的示例。

```
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強化指南

本指南[Cisco IOS XR軟體加固指南](#)可幫助網路管理員和安全從業人員保護基於Cisco IOS XR的路由器，以提高網路的整體安全狀態。

本文檔圍繞網路裝置功能分類的三個平面進行構建。

路由器的三個功能平面是管理平面、控制平面和資料平面。每個模組都提供必須保護的不同功能。

- **管理平面**：管理平面包含所有流量的邏輯組，這些流量支援Cisco IOS XR裝置和網路的調配、維護和監控功能。此組中的流量包括安全殼層(SSH)、安全複製通訊協定(SCP)、簡易網路管理通訊協定(SNMP)、系統日誌、TACACS+、RADIUS、DNS、NetFlow和思科探索通訊協定。管理平面流量總是發往本地Cisco IOS XR裝置。
- **控制平面**：控制平面包含用於建立和維護網路及其介面狀態的所有路由、信令、鏈路狀態和其他控制協定的邏輯組。這些技術包括邊界閘道通訊協定(BGP)、開放最短路徑優先(OSPF)、標籤發佈通訊協定(LDP)、中間系統到中間系統(IS-IS)、網路時間通訊協定(NTP)、位址解析通訊協定(ARP)和第2層keepalive。控制平面流量總是發往本地Cisco IOS XR裝置。
- **資料平面**：資料平面包含由主機、客戶端、伺服器 and 應用程式生成的「客戶」應用程式流量的邏輯組，這些流量源自網路支援的其它類似裝置，且目標為這些裝置。資料平面功能包括IP源路由、IP定向廣播、ICMP重定向、ICMP不可達和代理ARP。資料平面流量主要通過快速路徑轉發，從不發往本地Cisco IOS XR裝置。

Config Resilient Infrastructure Tester

您可以測試路由器配置，以便檢視它是否安全。該工具適用於多種作業系統，包括IOS XR:[Cisco Config Revistable Infrastructure Tester](#)。

版本和一般資料

1.如果再次配置命令或再次配置同一命令，它是否再次觸發同一系統日誌警告消息？

A:編號

2.同一提交中兩個不同功能的兩個配置命令是否會導致兩個系統日誌警告？

A:會。

範例：

```
RP/0/RP0/CPU0:Oct 17 19:01:48.806 UTC:ipv6_io[310]:%INFRA-WARN_INSECURE-4-
INSECURE_FEATURE_WARN :已使用或配置功能「IPV6源路由」。此功能已知不安全，請考慮
停止使用此功能。由於存在安全風險，請不要啟用IPv6源路由。
```

```
RP/0/RP0/CPU0:Oct 17 19:01:48.806 UTC:ipv4_ma[254]:%INFRA-WARN_INSECURE-4-
```

INSECURE_FEATURE_WARN :已使用或配置功能「IPv4源路由」。此功能已知不安全，請考慮停止使用此功能。由於安全風險，請勿啟用IPv4源路由。

3.新提交中的新的不安全配置命令是否會引發新的警告？

A:會。

4.從配置中刪除不安全的功能時，是否出現系統日誌警告？

A:是

範例:

RP/0/RP0/CPU0:Oct 18 08:16:24.410 UTC:ssh_conf_proxy[1210]:%INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED:已刪除不安全功能「SSH host-key DSA algorithm」配置。

RP/0/RP0/CPU0:Oct 22 06:37:21.960 UTC:tacacsd[115]:%INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED:已刪除不安全功能「TACACS+共用金鑰 (型別7編碼)」配置。

RP/0/RP0/CPU0:Oct 22 06:42:21.805 UTC:tacacsd[115]:%INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED:已刪除不安全功能「TACACS+ over TCP with shared secret(default mode)(使用共用金鑰 (預設模式) 的TACACS+)配置。

5.您看不到路由器上有Telnet可用。

A:您可以運行IOS XR XR7/LNT，它僅在載入可選Telnet RPM時才有Telnet可用。

6.您看不到XR7/LNT具有命令「install source」的sFTP或SCP選項。

A:目前，XR7/LNT不支援「install source」命令的sFTP或SCP。

7.更改是否同樣適用於IOS XR eXR和IOS XR XR7/LNT？

A:會。

8.如何檢查路由器是否運行IOS XR eXR或IOS XR XR7/LNT

A:使用「show version」並尋找「LNT」。8000路由器和一些NCS540變體運行IOS XR XR7/LNT。

範例：

<#root>

RP/0/RP0/CPU0:Router#

show version

Cisco IOS XR Software, Version 25.2.2

LNT

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。