思科IOS XR弹性基础设施

目录

简介

思科IOS XR弹性基础设施

- 受影响的功能
- 分组
  - 阶段
- 警告阶段
- 已弃用的不安全选项列表
  - IP源路由(RFC 791)
  - SSH v1
  - 使用预共享密钥的TACACS+和Radius（第7类）
  - TLS 1.0/1.1，弃用弱密码
  - Telnet（服务器和客户端）
  - TFTP（服务器和客户端）
  - TCP/UDP小型服务器
  - FTP
  - SNMP v1/2c
  - NTP版本2和3以及MD5身份验证
  - GRPC
  - 3DES-CBC密码
  - Diffie-Hellman组1 SHA1密钥交换
- 不安全的执行命令列表
  - 复制命令
  - 安装命令
  - 加载命令
  - 实用程序命令
- 杨氏模特
- 第 2 阶段
  - Telnet限制
  - TFTP、FTP和RCP功能限制
  - 安装限制

IOS XR强化指南

配置弹性基础设施测试器

问与答

简介

本文档介绍Cisco IOS® XR的一个加强方面:系统地逐步消除不安全的功能和密码。

思科IOS XR弹性基础设施

为了提高思科设备的安全状态，思科正在更改默认设置，弃用并最终删除不安全的功能，并引入新的安全功能。这些更改旨在增强您的网络基础设施，并提供对威胁发起者活动的更佳可视性。

请仔细阅读此信任中心页面：可恢复的基础设施。其中提到了基础设施强化、Cisco IOS XR软件强化指南、功能弃用过程以及功能弃用和删除详细信息。此处提及了建议的替代方案：功能删除和建议的替代方案。

Cisco IOS XR正在逐步消除不安全的功能和密码。这包括Cisco IOS XR中的配置命令和执行命令。

受影响的功能

- Telnet
- TFTP
- FTP
- HTTP
- SNMP v1/v2c
- 不带authPriv的SNMP v3
- IP源路由
- TCP/UDP小型服务器
- 使用预共享密钥（类型7）和MD5的TACACS+和Radius
- SSH v1
- TLS 1.0/1.1
- NTPv2/3和MD5
- GRPC，无TLS，TLSv1.0/1.1
- 使用copy、utility和install与TFTP/FTP执行命令

分组

有配置命令，但也有执行命令（例如“copy”命令）。

已弃用的命令可以分组：

- SSHv1、Telnet（服务器和客户端）、TFTP（客户端）、FTP
- DSA主机密钥，TACACS/RADIUS类型7,TLS 1.0/1.1
- 其他：TCP/UDP小型服务器，IP源路由（IPv4和IPv6）

阶段

此项目遵循通常的功能弃用方法：警告 — >限制 — >删除。

- Cisco IOS XR 25.4.1版中的警告。
- 限制阶段
- 功能删除

警告阶段

警告是什么？

1. CLI（命令行界面）帮助功能
2. 系统日志警告
3. Yang模块中的描述警告

对配置的不安全选项发出警告。这些是频率为30天的系统日志消息。

当使用任何不安全的功能时，会发出以下日志警告（级别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，请考虑停止使用此功能。<建议>

建议使用什么来代替不安全选项。

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，请考虑停止使用此功能。建议使用*SFTP*。

注意所用或配置的字词。使用指执行命令，配置指配置命令。

如果删除了不安全的选项（级别6或信息性），则会显示警告消息。 示例：

*RP/0/RP0/CPU0:Oct 22 06:43:43.967 UTC:tacacsd[1155]:%INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED :*已删除不安全功能“*TACACS+ over TCP with shared secret(default mode)*（基于共享密钥的*TACACS+ [*默认模式]）”配置。

已弃用的不安全选项列表

这是触发警告阶段的Cisco IOS XR版本中的警告的不安全选项列表。

该列表显示了不安全的选项、配置或执行命令、警告消息和关联的Yang模型。

IP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 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源路由

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，请考虑停止使用此功能。由于存在安全风险，请勿启用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，请考虑停止使用此功能。由于存在安全风险，请勿启用IPv6源路由。

Yang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

建议

删除不安全的选项。

不存在确切的替代方案。希望根据源地址控制网络流量的客户可以使用基于策略的路由或其他管理员控制的源路由机制（不将路由决策留给最终用户）进行控制。

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
RP/0/RP0/CPU0:Router(config)#
ssh server ?

  v1                          Cisco sshd protocol version 1. This is deprecated in 25.3.1.
```

ssh客户端v1

ssh服务器v1

警告

RP/0/RP0/CPU0:Nov 19 15:20:42.814 UTC:ssh_conf_proxy[1210]:%SECURITY-SSHD_CONF_PRX-4-WARNING_GENERAL :此平台和版本不支持备份服务器、netconf-port配置、ssh v1、ssh端口，这些配置不会生效

Yang模型

Cisco-IOS-XR-um-ssh-cfg

建议

使用SSH v2。

配置SSHv2：实施安全外壳

使用预共享密钥的TACACS+和Radius（第7类）

CLI

<#root>

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

tacacs-server host 10.0.0.1

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

key ?

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

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

tacacs-server key ?

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

tacacs-server key 7 135445410615102B28252B203E270A

tacacs-server host 10.1.1.1 port 49

密钥7 1513090F007B7977

radius-server host 10.0.0.1 auth-port 9999 acct-port 888

密钥7 1513090F007B7977

aaa server radius dynamic-author

client 10.10.10.2 vrf default

server-key 7 05080F1C2243

radius-server key 7 130415110F

aaa group server radius RAD

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

密钥7 1304464058

警告

RP/0/RP0/CPU0:Oct 18 18:00:42.505 UTC:tacacsd[1155]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN :已使用或配置功能“TACACS+共享密钥（类型7编码）”。此功能已知不安全，请考虑停止使用此功能。使用类型6（基于AES）加密。

RP/0/RP0/CPU0:Oct 18 18:00:42.505 UTC:tacacsd[1155]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN :已使用或配置功能“TACACS+ over TCP with shared secret(default mode)”。此功能已知不安全，请考虑停止使用此功能。使用基于TLS的TACACS+（安全TACACS+）实现更强的安全性。

RP/0/RP0/CPU0:Oct 18 18:18:19.460 UTC:radiusd[1149]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN :已使用或配置功能“RADIUS共享密钥（类型7编码）”。此功能已知不安全，请考虑停止使用此功能。使用类型6（基于AES）加密。

RP/0/RP0/CPU0:Oct 18 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（默认模式）”。此功能已知不安全，请考虑停止使用此功能。使用RADIUS over

TLS(RadSec)或DTLS以增强安全性。

Yang模型

-

建议

使用TACACS+或TLS 1.3或DTLS上的Radius。使用类型6作为凭证。

配置基于TLS 1.3或DTLS的TACACS+或Radius：配置AAA服务

TLS 1.0/1.1，弃用弱密码

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

-

Yang模型

Cisco-IOS-XR-um-logging-cfg

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

建议

使用TLS1.2或TLS1.3。

配置安全日志记录：实施安全日志

Telnet（服务器和客户端）

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 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 recon
  server  Telnet server configuration commands. (Telnet is deprecated since 25.4.1. SSH is recon

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 recon
  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

警告

RP/0/RP0/CPU0:Jun 27 10:59:52.226 UTC:cinetd[145]:%IP-CINETD-4-TELNET_WARNING:从25.4.1开始，不再支持Telnet。请改用SSH。

Yang模型

Cisco-IOS-XR-ipv4-telnet-cfg

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

Cisco-IOS-XR-um-telnet-cfg

建议

使用SSHv2。

配置SSHv2：实施安全外壳

TFTP（服务器和客户端）

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客户端

警告

RP/0/RP0/CPU0:Oct 17 19:03:29.475 UTC:tftp_fs[414]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN :已使用或配置功能“TFTP客户端”。此功能已知不安全，请考虑停止使用此功能。请改用SFTP。

Yang模型

-

建议

使用sFTP或HTTPS。

配置sFTP：实施安全外壳

TCP/UDP小型服务器

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)
```

服务ipv4

服务IPv6

警告

-

Yang模型

Cisco-IOS-XR-ip-tcp-cfg

Cisco-IOS-XR-ip-udp-cfg

建议

禁用TCP/UDP小型服务器。

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 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

警告

RP/0/RP0/CPU0:Oct 16 21:42:42.897 UTC:ftp_fs[1190]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN :已使用或配置功能“FTP客户端”。此功能已知不安全，请考虑停止使用此功能。请改用SFTP。

Yang模型

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

建议

使用sFTP或HTTPS。

配置sFTP：实施安全外壳

SNMP v1/2c

CLI

<#root>

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

snmp-server ?


  chassis-id            String to uniquely identify this chassis
  community             Enable SNMP;  set community string and access privileges. (This is depr

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

snmp-server ?


  community             Enable SNMP;  set community string and access privileges. (This is depr

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

snmp-server user test test ?


  v1      user using the v1 security model (This is deprecated since 25.4.1)
  v2c     user using the v2c security model (This is deprecated since 25.4.1)
  v3      user using the v3 security model

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

snmp-server host 10.0.0.1 version ?


  1   Use 1 for SNMPv1. (This is deprecated since 25.4.1)
  2c  Use 2c for SNMPv2c. (This is deprecated since 25.4.1)
  3   Use 3 for SNMPv3

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

snmp-server group test ?
```

```
  v1   group using the v1 security model (This is deprecated since 25.4.1)
  v2c  group using the v2c security model (This is deprecated since 25.4.1)
  v3   group using the User Security Model (SNMPv3)

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

snmp-server ?


  community             Enable SNMP;  set community string and access privileges. (This is depr
  community-map         Community Mapping as per RFC-2576. (This is deprecated since 25.4.1)

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

snmp-server user user1 group1 ?


  v1      user using the v1 security model (This is deprecated since 25.4.1)
  v2c     user using the v2c security model (This is deprecated since 25.4.1)

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

snmp-server user user1 group1 v3 auth md5 test priv ?


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

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

snmp ?


  community             Enable SNMP;  set community string and access privileges. (This is depr

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

snmp user user test ?


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

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

snmp-server user user1 group1 v3 auth ?


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

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

```
snmp user user1 group1 v3 auth ?


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

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

snmp user user1 group1 v3 auth md5 test priv ?


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

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

snmp host 10.1.1.1 version ?


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

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

snmp-server host 10.1.1.1 version ?


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

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

snmp ?


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

snmp-server community

snmp-server user <> <> v1 | v2c

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

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

snmp-server host <>版本1|v2c

snmp-server group <> v1|v2c

snmp-server community-map

SNMP社区

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

-

Yang模型

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

建议

将SNMPv3与身份验证和加密(authPriv)配合使用。

配置SNMPv3 with authentication and authPriv：配置简单网络管理协议。

NTP版本2和3以及MD5身份验证

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 <>广播版本2|3

ntp interface <>组播版本2|3

ntp authentication-key <> md5 <> <>

警告

RP/0/RP0/CPU0:Nov 25 16:09:15.422 UTC:ntpd[159]:%IP-IP_NTP-5-CONFIG_NOT_RECOMMENDED :从25.4.1开始，NTPv2和NTPv3被弃用。请使用NTPv4。

RP/0/RP0/CPU0:Nov 25 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，请考虑停止使用此功能。

Yang模型

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

建议

使用NTP第4版或除MD5以外的身份验证。

配置NTP：配[置网络时间协议]

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（在TLS 1.2中，在评估三个配置后使用不安全密码套件时是不安全的）

警告

RP/0/RP0/CPU0:Nov 29 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”。此功能已弃用，因为它被认为不安全；在以后的版本中将删除它。server=DEFAULT（TLS版本早于1.2，配置了不安全的密码套件）

Yang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

建议

使用具有强密码的TLS 1.2或更高版本（最好是TLS 1.3）。

配置：使用gRPC协议定义数据模型的网络操作

3DES-CBC密码

CLI

```
RP/0/RP0/CPU0:Router(config)#ssh server enable cipher ?
  3des-cbc Enable ssh server 3des-cbc algorithm. This is deprecated from 25.4.1
  aes-cbc Enable ssh server aes-cbc algorithms

RP/0/RP0/CPU0:Router(config)#ssh client enable cipher ?
  3des-cbc Enable ssh client 3des-cbc algorithm. This is deprecated from 25.4.1
  aes-cbc Enable ssh client aes-cbc algorithms
```

<#root>

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

ssh server algorithms cipher ?


WORD choose one or more in required preference
aes128-ctr
aes192-ctr
aes256-ctr
aes128-gcm@openssh.com
aes256-gcm@openssh.com
aes128-cbc
aes192-cbc
aes256-cbc
3des-cbc (This is deprecated from 25.4.1)
chacha20-poly1305@openssh.com

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

```
ssh client algorithms cipher ?


WORD choose one or more in required preference
aes128-ctr
aes192-ctr
aes256-ctr
aes128-gcm@openssh.com
aes256-gcm@openssh.com
aes128-cbc
aes192-cbc
aes256-cbc
3des-cbc (This is deprecated from 25.4.1)
  chacha20-poly1305@openssh.com
```

SSH服务器启用密码3des-cbc
SSH服务器算法密码3des-cbc
SSH服务器算法密钥交换diffie-hellman-group1-sha1

SSH客户端启用密码3des-cbc
SSH客户端算法密码3des-cbc
SSH客户端算法密钥交换diffie-hellman-group1-sha1

警告

RP/0/RP0/CPU0:Jun 3 07:11:48.212 UTC:ssh_conf_proxy[1210]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN :已使用或配置功能“3DES-CBC for SSH client cipher algorithm list”。此功能已弃用，因为它被认为不安全；在以后的版本中将删除它。

RP/0/RP0/CPU0:Jun 3 07:16:54.913 UTC:ssh_conf_proxy[1210]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN :已使用或配置功能“3DES-CBC for SSH server cipher algorithm list”。此功能已弃用，因为它被认为不安全；在以后的版本中将删除它。

Yang模型

Cisco-IOS-XR-um-ssh-cfg

建议

使用安全密码。

Diffie-Hellman组1 SHA1密钥交换

CLI

```
RP/0/RP0/CPU0:Router(config)#ssh client algorithms key-exchange ?
  WORD choose one or more in required preference
        ecdh-sha2-nistp521
        ecdh-sha2-nistp384
        ecdh-sha2-nistp256
        diffie-hellman-group14-sha1
        diffie-hellman-group1-sha1 (This is deprecated from 25.4.1)
        curve25519-sha256
        diffie-hellman-group14-sha256
        diffie-hellman-group16-sha512
        curve25519-sha256@libssh.org

RP/0/RP0/CPU0:Router(config)#ssh server algorithms key-exchange ?
  WORD choose one or more in required preference
        ecdh-sha2-nistp521
        ecdh-sha2-nistp384
        ecdh-sha2-nistp256
        diffie-hellman-group14-sha1
        diffie-hellman-group1-sha1 (This is deprecated from 25.4.1)
        curve25519-sha256
        diffie-hellman-group14-sha256
        diffie-hellman-group16-sha512
       curve25519-sha256@libssh.org
```

警告

RP/0/RP0/CPU0:Jun 3 10:00:03.566 UTC:ssh_conf_proxy[1210]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN :已使用或配置功能“Diffie Hellman Group1 SHA1 for SSH client Key Exchange”。此功能已弃用，因为它被认为不安全；在以后的版本中将删除它。

RP/0/RP0/CPU0:Jun 3 10:02:53.874 UTC:ssh_conf_proxy[1210]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN :已使用或配置功能“Diffie Hellman Group1 SHA1 for SSH Server Key Exchange”。此功能已弃用，因为它被认为不安全；在以后的版本中将删除它。

Yang模型

Cisco-IOS-XR-um-ssh-cfg

建议

使用安全密钥交换算法。

不安全的执行命令列表

复制命令

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)
```

<#root>

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

copy running-config ?

```
  ftp:       Copy to ftp: file system (Deprecated since 25.4.1)
  tftp:      Copy to tftp: file system (Deprecated since 25.4.1)
```

copy <src as tftp/ftp> <dst as tftp/ftp>

copy running-config <tftp/ftp>

copy <tftp/ftp> running-config

警告

RP/0/RP0/CPU0:Nov 26 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”。此功能已弃用，因为它被认为不安全；在以后的版本中将删除它。请改用SFTP或SCP。

RP/0/RP0/CPU0:Nov 26 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”。此功能已弃用，因为它被认为不安

全；在以后的版本中将删除它。请改用SFTP或SCP。

Yang模型

-

建议

使用sFTP或SCP。

配置：实施安全外壳

安装命令

CLI

```
install source

install add source

install replace
```

"

警告

-

Yang模型

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

建议

使用sFTP或SCP。

配置：实施安全外壳

加载命令

CLI

<#root>

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

configure

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

load ?

```
  ftp:           Load from ftp: file system (Deprecated since 25.4.1)
  tftp:          Load from tftp: file system (Deprecated since 25.4.1)
```

<#root>

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

load script ?

```
  ftp:       Load from ftp: file system (Deprecated since 25.4.1)
  tftp:      Load from tftp: file system (Deprecated since 25.4.1)
```

<#root>

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

load diff ?

```
  ftp:       Load from ftp: file system (Deprecated since 25.4.1)
  tftp:      Load from tftp: file system (Deprecated since 25.4.1)
```

<#root>

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

load diff reverse ?

```
  ftp:       Load from ftp: file system (Deprecated since 25.4.1)
  tftp:      Load from tftp: file system (Deprecated since 25.4.1)
```

load <ftp/tftp>

load script <ftp/tftp>

load diff <ftp/tftp>

load diff reverse <ftp/tftp>

警告

RP/0/RP0/CPU0:Dec 18 10:58:45.938 UTC:config[68291]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN :功能“load ftp:' used or configured”。此功能已弃用，因为它被认为不安全；在以后的版本中将删除它。通过ftp加载：不安全且已弃用。请改用scp或sftp。

RP/0/RP0/CPU0:Dec 18 10:58:51.584 UTC:config[68291]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN :已使用或配置功能“load tftp:'”。此功能已弃用，因为它被认为不安全；在以后的版本中将删除它。通过tftp加载：不安全且已弃用。请改用scp或sftp。

RP/0/RP0/CPU0:Dec 18 10:52:11.086 UTC:config[67526]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN :功能“load script ftp:' used or configured”。此功能已弃用，因为它被认为不安全；在以后的版本中将删除它。通过ftp加载脚本：不安全且已弃用。请改用scp或sftp。

RP/0/RP0/CPU0:Dec 18 10:53:38.825 UTC:config[68291]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN :已使用或配置功能“load script tftp:'”。此功能已弃用，因为它被认为不安全；在以后的版本中将删除它。通过tftp加载脚本：不安全且已弃用。请改用scp或sftp。

RP/0/RP0/CPU0:Dec 18 08:24:37.414 UTC:config[65969]:%INFRA-WARN_INSECURE-4-

INSECURE_FEATURE_WARN :功能“load diff ftp:' used or configured.此功能已弃用，因为它被认为不安全；在以后的版本中将删除它。正在加载diff over ftp:不安全且已弃用。请改用scp或sftp。

RP/0/RP0/CPU0:Dec 18 10:55:37.248 UTC:config[68291]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN :已使用或配置功能“load diff tftp:'”。此功能已弃用，因为它被认为不安全；在以后的版本中将删除它。正在加载diff over tftp:不安全且已弃用。请改用scp或sftp。

RP/0/RP0/CPU0:Dec 18 10:56:21.806 UTC:config[68291]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN :已使用或配置功能“load diff reverse ftp:'”。此功能已弃用，因为它被认为不安全；在以后的版本中将删除它。正在加载diff over ftp:不安全且已弃用。请改用scp或sftp。

RP/0/RP0/CPU0:Dec 18 10:56:12.031 UTC:config[68291]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN :已使用或配置功能“load diff reverse tftp:'”。此功能已弃用，因为它被认为不安全；在以后的版本中将删除它。正在加载diff over tftp:不安全且已弃用。请改用scp或sftp。

Yang模型

-

建议

使用sFTP或SCP。

配置：实施安全外壳

实用程序命令

CLI

```
utility mv source
```

```
utility mv source
```

```
       source
```

警告

RP/0/RP0/CPU0:Dec 18 10:30:22.499 UTC:run_utility[68509]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN :已使用或配置功能“utility mv tftp”。此功能已弃用，因为它被认为不安全；在以后的版本中将删除它。

RP/0/RP0/CPU0:Dec 18 10:30:35.803 UTC:run_utility[68549]:%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN :已使用或配置功能“utility mv ftp”。此功能已弃用，因为它被认为不安全；在以后的版本中将删除它。

Yang模型

-

建议

使用sFTP或SCP。

配置：实施安全外壳

杨氏模特

Yang型号中有太多更改，无法在此处列出所有更改。

以下是Yang模型*Cisco-IOS-XR-ipv4-ma-cfg.yangan*中用于删除源路由的注释的示例。

```
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 *modelCisco-IOS-XR-um-ftp-tftp-cfg*.yang中用于删除FTP和TFTP的注释的示例。

```
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)";
```

第 2 阶段

在IOS XR版本26.2.1中，有4项功能被移入限制阶段：Telnet、FTP、TFTP和RCP。

Telnet、FTP、TFTP和RCP配置和执行命令已受到限制。有关受限命令的完整列表，请参阅配置和执行命令的不安全功能部分。

将Telnet添加到可选RPM Telnet.rpm，并将FTP、TFTP和RCP添加到可选RPM IP-Insecure-Apps.rpm。

使用现有的不安全配置升级的路由器可能会发出配置不一致警报。在提交任何新配置之前，必须清除不一致。

```
<#root>

RP/0/RP0/CPU0:Router#

conf t


In this SDR's running configuration is inconsistent with persistent configuration.
No configuration commits for this SDR will be allowed until a '

clear configuration inconsistency

' command is performed.
```

Telnet限制

Telnet配置和执行命令将移至可选RPM:Telnet.rpm。

如果尚未安装telnet.rpm，则仍支持通过Telnet连接到控制台端口（和aux端口）。

如果已安装Telnet.rpm且配置为“telnet ipv4 client source-interface mgmth 0/RP0/CPU0”，则仍支持通过Telnet连接到管理端口。

自7.0.1起，Telnet已是Lindt平台的可选RPM，因此不会对Lindt平台进行更改。

只要配置了不安全功能，系统仍会每30天发出一次系统日志警告。

以下yang型号受到影响。

Cisco-IOS-XR-ipv4-telnet-cfg

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

Cisco-IOS-XR-um-telnet-cfg

TFTP、FTP和RCP功能限制

TFTP、FTP和RCP配置和执行命令将移至可选RPM:IP-Insecure-Apps.rpm。

只要配置了不安全功能，系统仍会每30天发出一次系统日志警告。

此限制仅适用于eXR。计划在未来版本中使用Lindt限制。

如果未安装IP-Insecure-apps.rpm可选rpm，则不接受以下包含TFTP/FTP/RCP的命令：

- 复制
- 公用事业
- 负载
- install（安装）
- 脚本添加

如果使用不安全的协议，则会显示错误。例如：

```
Error : Install operation using FTP is deprecated as it is known to be insecure. FTP is currently part
```

以下yang型号受到影响。

- Cisco-IOS-XR-um-ftp-tftp-cfg
- Cisco-IOS-XR-ip-tcp-cfg
- Cisco-IOS-XR-shellutil-copy-act

安装限制

安装命令将移至可选的RPM IP-Insecure-Apps.rpm。

```
<#root>

RP/0/RP0/CPU0:Router#

install add source ftp://cisco@10.1.1.1/tftpboot telnet.rpm

Error : Install operation using FTP is deprecated as it is known to be insecure. FTP is currently part
```

IOS XR强化指南

本指南Cisco IOS XR软件加固指南可帮助网络管理员和安全从业人员保护基于Cisco IOS XR的路由器的安全，从而提高网络的整体安全状态。

本文档围绕网络设备功能分类的三个平面进行构建。

路由器的三个功能平面是管理平面、控制平面和数据平面。每个模块都提供必须保护的不同功能。

- **管理平面**：管理平面包含支持思科IOS XR设备和网络的调配、维护和监控功能的所有流量的逻辑组。此组中的流量包括安全外壳(SSH)、安全复制协议(SCP)、简单网络管理协议(SNMP)、系统日志、TACACS+、RADIUS、DNS、NetFlow和思科发现协议。管理平面流量始终指向本地思科IOS XR设备。
- **控制平面：控制平面包含所有路由、信令、链路状态和其他控制协议的逻辑组，这些协议用于创建和维护网络及其接口的状态。这些协议包括边界网关协议(BGP)、开放最短路径优先(OSPF)、标签分发协议(LDP)、中间系统到中间系统(IS-IS)、网络时间协议(NTP)、地址解析协议(ARP)和第2层keepalive。控制平面流量始终流向本地思科IOS XR设备。**
- **数据平面：数据平面包含由主机、客户端、服务器和应用程序生成的“客户”应用流量逻辑组，这些流量来自网络支持的其它类似设备，并且发往这些设备。数据平面功能包括IP源路由、IP定向广播、ICMP重定向、ICMP不可达和代理ARP。数据平面流量主要通过快速路径转发，并且不会发往本地Cisco IOS XR设备。**

配置弹性基础设施测试器

您可以测试路由器配置，以查看它是否安全，该工具适用于多种操作系统，包括IOS XR:Cisco Config Resilient Infrastructure Tester。

问与答

1.如果第二次配置命令或再次配置同一命令，是否会再次触发同一系统日志警告消息？

A：No.

2.同一提交中两个不同功能的两个配置命令是否会导致两个系统日志警告？

A：Yes.

示例：

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，请考虑停止使用此功能。由于存在安全风险，请勿启用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，请考虑停止使用此功能。由于存在安全风险，请勿启用IPv4源路由。

3.新的提交中新的不安全配置命令是否会引发新的警告？

A：Yes.

4.当从配置中删除不安全的功能时，是否出现系统日志警告？

A：Yes

示例：

RP/0/RP0/CPU0:Oct 18 08:16:24.410 UTC:ssh_conf_proxy[1210]:%INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED :已删除不安全功能“SSH主机密钥DSA算法”配置。

RP/0/RP0/CPU0:Oct 22 06:37:21.960 UTC:tacacsd[1155]:%INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED :已删除不安全功能“TACACS+共享密钥（类型7编码）”配置。

RP/0/RP0/CPU0:Oct 22 06:42:21.805 UTC:tacacsd[1155]:%INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED :已删除不安全功能“TACACS+ over TCP with shared secret(default mode)（基于共享密钥的TACACS+ [默认模式]）”配置。

5.您看不到路由器上有Telnet可用。

A：您可以运行IOS XR XR7/LNT，只有当您加载可选Telnet RPM时，IOS XR XR7/LNT才提供Telnet。

6.您不会看到XR7/LNT具有“install source”命令的sFTP或SCP选项。

A：目前，XR7/LNT不支持“install source”命令的sFTP或SCP。

7.更改是否同样适用于IOS XR eXR和IOS XR XR7/LNT?

A：Yes.

8.如何检查路由器是否运行IOS XR eXR或IOS XR XR7/LNT

A：使用“show version”并查找“LNT”。8000路由器和一些NCS540变体运行IOS XR XR7/LNT。

示例：

```
<#root>
RP/0/RP0/CPU0:Router#
show version

Cisco IOS XR Software, Version 25.2.2
LNT
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。