인프라 탄력성 Cisco IOS XR

목차

소개

이 문서에서는 Cisco IOS® XR의 한 가지 강화 측면에 대해 설명합니다. 보안되지 않은 기능과 암호를 체계적으로 단계적으로 제거합니다.

Cisco IOS XR 인프라 복원력

Cisco는 Cisco 장치의 보안 상태를 개선하기 위해 기본 설정을 변경하고, 안전하지 않은 기능을 사용 중지했다가 결국에는 제거하고, 새로운 보안 기능을 도입하고 있습니다. 이러한 변경은 네트워크 인프라를 강화하고 위협 행위자 활동에 대한 더 나은 가시성을 제공하기 위해 설계되었습니다.

이 Trust Center 페이지, 즉 Resilient Infrastructure를 살펴보십시오. 인프라 강화, Cisco IOS XR Software Hardening Guide, 기능 사용 중단 프로세스, 기능 사용 중단 및 제거 세부 사항에 대해 설명합니다. 제안 된 대안은 여기에 언급 됩니다: 기능 제거 및 제안 된 대안.

Cisco IOS XR는 안전하지 않은 기능과 암호를 단계적으로 축소하고 있습니다. 여기에는 Cisco IOS XR의 configuration 및 execute 명령이 모두 포함됩니다.

영향을 받는 기능

- Telnet
- TFTP
- FTP
- HTTP
- SNMP v1/v2c
- authPriv가 없는 SNMP v3
- IP 소스 경로
- TCP/UDP 소규모 서버
- 사전 공유 키가 있는 TACACS+ 및 Radius(유형 7) 및 MD5
- SSH v1
- TLS 1.0/1.1
- NTPv2/3 및 MD5
- GRPC no TLS, TLSv1.0/1.1
- copy, utility 및 install with TFTP/FTP를 사용하는 EXEC 명령

그룹화

컨피그레이션 명령이 있지만 명령(예: "copy" 명령)도 실행합니다.

사용되지 않는 명령은 그룹화할 수 있습니다.

- SSHv1, 텔넷(서버 및 클라이언트), TFTP(클라이언트), FTP
- DSA 호스트 키, TACACS/RADIUS 유형 7, TLS 1.0/1.1
- 기타: TCP/UDP 소규모 서버, IP 소스 라우팅(IPv4 및 IPv6)

단계

이 프로젝트는 일반적인 기능 사용 중단 접근 방식을 따릅니다. 경고 -> 제한 -> 제거.

- Cisco IOS XR 릴리스 25.4.1의 경고.
- 제한 단계
- 기능 제거

경고 단계

경고문은 무엇입니까?

1. CLI(Command Line Interface) 도움말 기능
2. syslog 경고
3. yang 모듈의 설명 경고

구성된 비보안 옵션에 대해 경고가 표시됩니다. 빈도가 **30일인 syslog 메시지입니다**.

비보안 기능이 사용되는 경우 다음 로그 경고(수준 4 또는 경고)가 발생합니다.

*%**INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN**:* 기능 '<*feature-name*>'이(가) 사용되었거나 구성되었습니다. 이 기능은 안전하지 않은 것으로 알려져 있습니다. 이 기능의 사용을 중지하십시오. <권장 사항>

안전하지 않은 옵션 대신 어떤 옵션을 사용할지 권장합니다.

FTP에 대한 경고 예:

%INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: 'FTP' 기능이 사용되었거나 구성되었습니다. 이 기능은 안전하지 않은 것으로 알려져 있습니다. 이 기능의 사용을 중지하십시오. *SFTP*를 사용하는 것이 좋습니다.

사용 또는 구성된 단어를 확인합니다. Utilized는 execute 명령을 참조하고, configured는 configuration 명령을 참조합니다.

insecure 옵션이 제거된 경우 경고 메시지가 인쇄될 수 있습니다(수준 6 또는 정보). 예:

*RP/0/RP0/CPU0:10*월 22일 06:43:43.967 *UTC: tacacsd[1155]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED:* 비보안 기능 '공유 암호가 있는 *TCP*를 통한 *TACACS+(*기본 모드)' 컨피그레이션이 제거되었습니다.

사용되지 않는 비보안 옵션 목록

경고 단계의 Cisco IOS XR 릴리스에서 경고를 트리거하는 비보안 옵션 목록입니다.

목록에는 insecure 옵션, 컨피그레이션 또는 실행 명령, 경고 메시지 및 관련 Yang 모델이 표시됩니다.

IP 소스 라우팅(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 소스 경로

ipv6 소스 경로

ipv4 소스 경로

경고

RP/0/RP0/CPU0:10월 17일 19:01:48.806 UTC: ipv4_ma[254]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: 'IPV4 SOURCE ROUTE' 기능이 사용되었거나 구성되었습니다. 이 기능은 안전하지 않은 것으로 알려져 있습니다. 이 기능의 사용을 중지하십시오. 보안 위험 때문에 IPv4 소스 라우팅을 활성화하지 마십시오.

RP/0/RP0/CPU0:10월 17일 19:01:48.806 UTC: ipv6_io[310]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: 'IPV6 소스 경로' 기능이 사용되었거나 구성되었습니다. 이 기능은 안전하지 않은 것으로 알려져 있습니다. 이 기능의 사용을 중지하십시오. 보안 위험 때문에 IPv6 소스 라우팅을 활성화하지 마십시오.

양 모형

Cisco-IOS-XR-ipv4-ma-cfg

Cisco-IOS-XR-ipv6-io-cfg

Cisco-IOS-XR-um-ipv4-cfg

Cisco-IOS-XR-um-ipv6-cfg

권장 사항

안전하지 않은 옵션을 제거합니다.

정확한 대안이 존재하지 않습니다. 소스 주소를 기반으로 네트워크를 통과하는 트래픽을 제어하려는 고객은 최종 사용자에게 라우팅 결정을 맡기지 않는 정책 기반 라우팅 또는 기타 관리자가 제어하는 소스 라우팅 메커니즘을 사용하여 이러한 작업을 수행할 수 있습니다.

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 클라이언트 v1

ssh 서버 v1

경고

RP/0/RP0/CPU0:11월 19일 15:20:42.814 UTC: ssh_conf_proxy[1210]: %SECURITY-SSHD_CONF_PRX-4-WARNING_GENERAL: 백업 서버, netconf 포트 구성, ssh v1, ssh 포트는 이 플랫폼과 릴리스에서 지원되지 않으며 적용되지 않습니다

양 모형

Cisco-IOS-XR-um-ssh-cfg

권장 사항

SSH v2를 사용합니다.

컨피그레이션 SSHv2: Secure Shell 구현

사전 공유 키가 있는 TACACS+ 및 Radius(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-server key 7 135445410615102B28252B203E270A

tacacs-server 호스트 10.1.1.1 포트 49

키 7 1513090F007B7977

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

키 7 1513090F007B7977

aaa 서버 radius 동적 작성자

클라이언트 10.10.10.2 vrf 기본값

서버 키 7 05080F1C2243

radius-server key 7 130415110F

aaa 그룹 서버 반경 RAD

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

키 7 1304464058

경고

RP/0/RP0/CPU0:10월 18일 18:00:42.505 UTC: tacacsd[1155]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: 'TACACS+ 공유 암호(Type 7 인코딩)' 기능을 사용하거나 구성했습니다. 이 기능은 안전하지 않은 것으로 알려져 있습니다. 이 기능의 사용을 중지하십시오. 대신 Type 6(AES 기반) 암호화를 사용합니다.

RP/0/RP0/CPU0:10월 18일 18:00:42.505 UTC: tacacsd[1155]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: '공유 암호가 있는 TCP를 통한 TACACS+(기본 모드)' 기능이 사용되었거나 구성되었습니다. 이 기능은 안전하지 않은 것으로 알려져 있습니다. 이 기능의 사용을 중지하십시오. 더 강력한 보안을 위해 TACACS+ over TLS(Secure TACACS+)를 사용합니다.

RP/0/RP0/CPU0:10월 18일 18:18:19.460 UTC: radiusd[1149]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: 기능 'RADIUS 공유 암호(유형 7 인코딩)'를 사용하거나 구성했습니다. 이 기능은 안전하지 않은 것으로 알려져 있습니다. 이 기능의 사용을 중지하십시오. 대신 Type 6(AES 기반) 암호화를 사용합니다.

RP/0/RP0/CPU0:10월 18일 18:18:19.460 UTC: radiusd[1149]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: '공유 암호가 있는 RADIUS over UDP(기본 모드)' 기능이 사용되었거나 구성되었습니다. 이 기능은 안전하지 않은 것으로 알려져 있습니다. 이 기능의 사용을 중지하십시오. 더 강력한 보안을 위해 RADIUS over TLS(RadSec) 또는 DTLS를 사용합니다.

양 모형

-

권장 사항

TACACS+ 또는 Radius over TLS 1.3 또는 DTLS를 사용합니다. 자격 증명에 유형 6을 사용합니다.

TACACS+ 또는 RADIUS over TLS 1.3 또는 DTLS 구성: AAA 서비스 구성

TLS 1.0/1.1, 약한 암호 사용 중단

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
```

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

경고

-

양 모형

Cisco-IOS-XR-um-logging-cfg

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

권장 사항

TLS1.2 또는 TLS1.3을 사용합니다.

컨피그레이션 보안 로깅: 보안 로깅 구현

텔넷(서버 및 클라이언트)

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 inste

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

`telnet ipv4 ?`

```
  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 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
```

텔넷

텔넷 ipv4

텔넷 ipv6

텔넷 vrf

경고

RP/0/RP0/CPU0:6월 27일 10:59:52.226 UTC: cinetd[145]: %IP-CINETD-4-TELNET_WARNING: 텔넷 지원은 25.4.1 이후부터 사용되

지 않습니다. 대신 SSH를 사용하십시오.

양 모형

Cisco-IOS-XR-ipv4-telnet-cfg

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

Cisco-IOS-XR-um-telnet-cfg

권장 사항

SSHv2를 사용합니다.

컨피그레이션 SSHv2: Secure Shell 구현

TFTP(서버 및 클라이언트)

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 클라이언트

경고

RP/0/RP0/CPU0:10월 17일 19:03:29.475 UTC: tftp_fs[414]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: 'TFTP 클라이언트' 기능이 사용되었거나 구성되었습니다. 이 기능은 안전하지 않은 것으로 알려져 있습니다. 이 기능의 사용을 중지하십시오. 대신 SFTP를 사용하십시오.

양 모형

-

권장 사항

sFTP 또는 HTTPS를 사용합니다.

컨피그레이션 sFTP: Secure Shell 구현

TCP/UDP 소규모 서버

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)
```

서비스 ipv4

서비스 ipv6

경고

-

양 모형

Cisco-IOS-XR-ip-tcp-cfg

Cisco-IOS-XR-ip-udp-cfg

권장 사항

TCP/UDP 소규모 서버를 비활성화합니다.

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

경고

RP/0/RP0/CPU0:10월 16일 21:42:42.897 UTC: ftp_fs[1190]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: 'FTP 클라이언트' 기능이 사용되었거나 구성되었습니다. 이 기능은 안전하지 않은 것으로 알려져 있습니다. 이 기능의 사용을 중지하십시오. 대신 SFTP를 사용하십시오.

양 모형

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

권장 사항

sFTP 또는 HTTPS를 사용합니다.

컨피그레이션 sFTP: Secure Shell 구현

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 커뮤니티

snmp 서버 사용자 **<> <>** v1 | v2c

snmp-server 사용자 **<> <>** v3 인증 md5 | sha

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

snmp-server host <> 버전 1|v2c

snmp 서버 그룹 **<>** v1|v2c

snmp-server community-map

snmp 커뮤니티

snmp 사용자 **<>** **<>** v1|v2c

snmp 사용자 **<>** **<>** v3 auth md5|sha

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

snmp 호스트 **<>** 버전 1|v2c

snmp 그룹 **<>** v1|v2c

snmp 커뮤니티 맵

경고

-

양 모형

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

권장 사항

인증 및 암호화(authPriv)와 함께 SNMPv3를 사용합니다.

인증 및 authPriv로 SNMPv3 구성: 단순 네트워크 관리 프로토콜 구성

NTP 버전 2 및 3, MD5 인증

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 서버 **<>** 버전 2|3

ntp peer **<>** 버전 2/3

ntp server admin-plane 버전 1/2/3

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

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

ntp authentication-key **<>** md5 **<>** **<>**

경고

RP/0/RP0/CPU0:11월 25일 16:09:15.422 UTC: ntpd[159]: %IP-IP_NTP-5-CONFIG_NOT_RECOMMENDED: NTPv2 및 NTPv3은 25.4.1 이상 더 이상 사용되지 않습니다. NTPv4를 사용하십시오.

RP/0/RP0/CPU0:11월 25일 16:09:15.422 UTC: ntpd[159]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: '인증 없는 NTP' 기능이 사용되었거나 구성되었습니다. 이 기능은 안전하지 않은 것으로 알려져 있습니다. 이 기능의 사용을 중지하십시오.

양 모형

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

권장 사항

NTP 버전 4 또는 MD5 이외의 인증을 사용합니다.

컨피그레이션 NTP: [Network Time Protocol 구성]

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 (TLS 1.2에서는 세 가지 구성을 평가한 후 안전하지 않은 암호 그룹을 사용하는 경우 안전하지 않음)

경고

RP/0/RP0/CPU0: 11월 29일 19:38:30.833 UTC: emsd[1122]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: 'gRPC 비보안 컨피그레이션' 기능이 사용되었거나 구성되었습니다. 이 기능은 안전하지 않은 것으로 알려져 있으므로 더 이상 사용되지 않습니다. 향후 릴리스에서 제거될 예정입니다. server=DEFAULT(TLS 버전이 1.2보다 오래됨, 안전하지 않은 암호 그룹이 구성됨)

양 모형

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

권장 사항

강력한 암호와 함께 TLS 1.2 이상(바람직하게는 TLS 1.3)을 사용합니다.

컨피그레이션: gRPC 프로토콜을 사용하여 데이터 모델로 네트워크 작업 정의

Insecure Execute 명령 목록

명령 복사

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 ?"

경고

RP/0/RP0/CPU0:11월 26일 15:05:57.666 UTC: filesys_cli[66940]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: 'copy ftp' 기능이 사용되었거나 구성되었습니다. 이 기능은 안전하지 않은 것으로 알려져 있으므로 더 이상 사용되지 않습니다. 향후 릴리스에서 제거될 예정입니다. 대신 SFTP 또는 SCP를 사용하십시오.

RP/0/RP0/CPU0:11월 26일 15:09:06.181 UTC: filesys_cli[67445]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: 'copy tftp' 기능이 사용되었거나 구성되었습니다. 이 기능은 안전하지 않은 것으로 알려져 있으므로 더 이상 사용되지 않습니다. 향후 릴리스에서 제거될 예정입니다. 대신 SFTP 또는 SCP를 사용하십시오.

양 모형

-

권장 사항

sFTP 또는 SCP를 사용합니다.

컨피그레이션: Secure Shell 구현

설치 명령

CLI

```
install source

install add source

install replace

        "
```

경고

-

양 모형

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

권장 사항

sFTP 또는 SCP를 사용합니다.

컨피그레이션: Secure Shell 구현

유틸리티 명령

CLI

```
utility mv source
```

Yang 모델

Yang 모델에는 변경 사항이 너무 많아 모두 여기에 나열할 수 없습니다.

소스 라우팅 제거에 대한 Yang 모델*Cisco-IOS-XR-ipv4-ma-cfg.yang*의 설명 예입니다.

```
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)";
```

다음은 FTP 및 TFTP를 제거하기 위한 Yang 모델 *Cisco-IOS-XR-um-ftp-tftp-cfg*.yang의 설명에 대한 예입니다.

```
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 강화 가이드

Cisco IOS XR Software Hardening Guide는 네트워크 관리자와 보안 실무자가 Cisco IOS XR 기반 라우터를 보호하여 네트워크의 전반적인 보안 상태를 개선하는 데 도움이 됩니다.

이 문서는 네트워크 디바이스의 기능을 분류하는 세 가지 플레인을 중심으로 구성됩니다.

라우터의 세 가지 기능 플레인은 관리 플레인, 제어 플레인 및 데이터 플레인입니다. 각각은 보호해야 하는 서로 다른 기능을 제공합니다.

- **관리 플레인:** 관리 플레인에는 Cisco IOS XR 디바이스 및 네트워크에 대한 프로비저닝, 유지 관리 및 모니터링 기능을 지원하는 모든 트래픽의 논리 그룹이 포함됩니다. 이 그룹의 트래픽에는 SSH(Secure Shell), SCP(Secure Copy Protocol), SNMP(Simple Network Management Protocol), Syslog, TACACS+, RADIUS, DNS, NetFlow 및 Cisco Discovery Protocol이 포함됩니다. 관리 플레인 트래픽은 항상 로컬 Cisco IOS XR 디바이스로 향합니다.
- **컨트롤 플레인:** 컨트롤 플레인에는 네트워크 및 해당 인터페이스의 상태를 만들고 유지하는 데 사용되는 모든 라우팅, 시그널링, 링크 상태 및 기타 컨트롤 프로토콜의 논리 그룹이 포함됩니다. 여기에는 BGP(Border Gateway Protocol), OSPF(Open Shortest Path First), LDP(Label Distribution Protocol), IS-IS(Intermediate System to Intermediate System), NTP(Network Time Protocol), ARP(Address Resolution Protocol) 및 레이어 2 킵얼라이브가 포함됩니다. 컨트롤 플레인 트래픽은 항상 로컬 Cisco IOS XR 디바이스로 전달됩니다.
- **데이터 플레인:** 데이터 플레인에는 네트워크에서 지원하는 유사한 다른 장치로 보내지고 전달되는 호스트, 클라이언트, 서버 및 애플리케이션에서 생성되는 "고객" 애플리케이션 트래픽의 논리적 그룹이 포함됩니다. 데이터 플레인 기능에는 IP 소스 라우팅, IP 지향 브로드캐스트, ICMP 리디렉션, ICMP 연결 불가능, 프록시 ARP가 포함됩니다. 데이터 플레인 트래픽은 주로 빠른 경로에서 포워딩되며 결코 로컬 Cisco IOS XR 디바이스로 향하는 것이 아닙니다.

Config Resilient Infrastructure Tester

IOS XR: Cisco Config Resilient Infrastructure Tester를 비롯한 여러 운영 체제에서 작동하는 이 툴을 사용하여 라우터 컨피그레이션이 안전한지 여부를 확인할 수 있습니다.

질문과 대답

1. 명령을 두 번째로 구성하거나 동일한 명령을 다시 구성하면 동일한 syslog 경고 메시지가 다시 트리거됩니까?

A : 아니요.

2. 동일한 커밋에서 서로 다른 두 기능에 대한 두 개의 컨피그레이션 명령으로 인해 두 개의 syslog 경고가 발생합니까?

A : 예.

예:

RP/0/RP0/CPU0:10월 17일 19:01:48.806 UTC: ipv6_io[310]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: 'IPV6 소스 경로' 기능이 사용되었거나 구성되었습니다. 이 기능은 안전하지 않은 것으로 알려져 있습니다. 이 기능의 사용을 중지하십시오. 보안 위험 때문에 IPv6 소스 라우팅을 활성화하지 마십시오.

RP/0/RP0/CPU0:10월 17일 19:01:48.806 UTC: ipv4_ma[254]: %INFRA-WARN_INSECURE-4-INSECURE_FEATURE_WARN: 'IPV4 SOURCE ROUTE' 기능이 사용되었거나 구성되었습니다. 이 기능은 안전하지 않은 것으로 알려져 있습니다. 이 기능의 사용을 중지하십시오. 보안 위험 때문에 IPv4 소스 라우팅을 활성화하지 마십시오.

3. 새로운 commit에서 새로운 비보안 컨피그레이션 명령으로 인해 새로운 경고가 발생합니까?

A : 예.

4. 비보안 기능이 컨피그레이션에서 제거될 때 syslog 경고가 표시됩니까?

A : 예

예:

RP/0/RP0/CPU0:10월 18일 08:16:24.410 UTC: ssh_conf_proxy[1210]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED: 비보안 기능 'SSH 호스트 키 DSA 알고리즘' 컨피그레이션이 제거되었습니다.

RP/0/RP0/CPU0:10월 22일 06:37:21.960 UTC: tacacsd[1155]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED: 안전하지 않은 기능 'TACACS+ 공유 암호(Type 7 인코딩)' 컨피그레이션이 제거되었습니다.

RP/0/RP0/CPU0:10월 22일 06:42:21.805 UTC: tacacsd[1155]: %INFRA-WARN_INSECURE-6-INSECURE_CONFIG_REMOVED: 비보안 기능 '공유 암호가 있는 TCP를 통한 TACACS+(기본 모드)' 컨피그레이션이 제거되었습니다.

5. 라우터에서 사용 가능한 텔넷이 표시되지 않습니다.

A : 선택 사항인 텔넷 RPM을 로드한 경우에만 텔넷이 제공되는 IOS XR XR7/LNT를 실행할 수 있습니다.

6. XR7/LNT에는 "install source" 명령에 대한 sFTP 또는 SCP 옵션이 표시되지 않습니다.

A : 현재 XR7/LNT는 "install source" 명령에 대해 sFTP 또는 SCP를 지원하지 않습니다.

7. 변경 사항이 IOS XR eXR 및 IOS XR XR7/LNT에도 동일하게 적용됩니까?

A : 예.

8. 라우터에서 IOS XR eXR을 실행하는지 IOS XR XR7/LNT를 실행하는지 어떻게 확인합니까?

A : "show version"을 사용하고 "LNT"를 찾습니다. 8000 라우터와 일부 NCS540 변형은 IOS XR7/LNT를 실행합니다.

예:

<#root>

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

Cisco IOS XR Software, Version 25.2.2
LNT
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.