Entender a infraestrutura resiliente em dispositivos IOS XE

Contents

Introdução

Este documento descreve a abordagem da Cisco para a infraestrutura resiliente, que está enraizada em segurança por padrão e segurança por design.

Pré-requisitos

Requisitos

Embora não haja requisitos específicos para este documento, um entendimento básico do software Cisco IOS ® XE é extremamente útil.

Componentes Utilizados

As informações neste documento são aplicáveis a todos os dispositivos que podem executar o software Cisco IOS XE 17.18.2 e posterior. Isso inclui roteadores, switches e WLCs do Cisco IOS XE.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Meta

Nosso objetivo é diminuir significativamente a superfície de ataque em produtos de rede da Cisco e minimizar as vulnerabilidades de segurança através de configurações padrão seguras, remoção de tecnologias e recursos herdados inseguros e segurança de produto aprimorada.

Você pode encontrar mais detalhes sobre a pressão na Cisco para melhorar a postura de segurança da rede na documentação da Infraestrutura resiliente, bem como no Guia de Fortalecimento do Software Cisco IOS XE. No entanto, este documento concentra-se principalmente nos aspectos técnicos e nas considerações que resultam da implementação em fases dessas alterações de segurança vitais.

Abordagem em fases

Para garantir uma superfície de ataque reduzida e a adoção de práticas recomendadas críticas de segurança, ao mesmo tempo em que minimiza a interrupção e o esforço de nossos clientes, a Cisco está adotando uma abordagem em fases para remover recursos e protocolos inseguros. Observe que a fase de configurações não seguras é específica de recursos ou protocolos. Um recurso pode permanecer na fase de Aviso enquanto outro recurso entra na fase de Restrição.

Fase um: Aviso

Os usuários recebem avisos na CLI quando configuram os principais recursos não seguros. Nossa meta é conscientizar os clientes sobre essas configurações inseguras para que eles possam começar a planejar a migração para opções mais seguras. A Cisco recomenda enfaticamente que todas as mensagens de aviso não seguras sejam tratadas imediatamente. As configurações não seguras na fase de Aviso não disparam nem exigem o Modo Não Seguro.

O Cisco IOS XE versão 17.18.2 é a primeira versão de software a introduzir a fase de Aviso para recursos não seguros.

Fase dois: Restrição

Os principais recursos não seguros são desativados por padrão e exigem ação explícita do usuário para ativá-los (através da introdução do Modo Não Seguro). As implantações existentes continuam a funcionar, mas novas instalações exigem a ativação intencional dessas configurações não seguras. Observe que alguns recursos nas plataformas Cisco IOS XE não podem ter uma fase de Restrição: eles podem

basta exibir avisos para várias versões antes de removê-las posteriormente.

O Cisco IOS XE versão 26.1.1 é a primeira versão de software a introduzir a fase de Restrição para recursos não seguros.

Fase três: Remoção

Os recursos obsoletos e inseguros são completamente removidos. O tempo de remoção do recurso varia, dependendo do impacto do usuário e da adoção. Por exemplo, os recursos amplamente adotados, como o SNMPv2, devem ser eliminados progressivamente mais lentamente do que os menos usados.

O Cisco IOS XE versão 26.2.1 é a primeira versão de software a introduzir a fase de Remoção para recursos não seguros.

Comandos-chave

Esses comandos são extremamente úteis à medida que os clientes implementam infraestruturas mais resilientes. Esses comandos são mencionados em todo este documento.

- show system unsecure configuration
  - Esse comando é usado para exibir as configurações não seguras atualmente aplicadas que estão na fase de Restrição. Ele não exibe configurações não seguras que estão na fase de Aviso ou de Remoção. Esse comando também exibe o tempo restante para a próxima verificação de configuração não segura (detalhado na seção Verificações de configuração não segura e Temporizadores).
- show system security mode
  - Este comando fornece uma breve saída que mostra se o dispositivo está no Modo de Segurança ou no Modo Inseguro.
- show running-config all | incluir modo de sistema inseguro
  - Esse comando exibe a configuração atual (incluindo as configurações padrão), filtrada nas palavras-chave insecure do modo de sistema. Consulte a seção Alterar Modo de Segurança para obter detalhes adicionais.
- test system secure all
  - Esse comando executa imediatamente uma verificação de configuração não segura e exibe a saída do comando show system insecure configuration. Isso é útil para atualizar as configurações sinalizadas sem segurança após uma alteração sem esperar que o temporizador de verificação expire.
- show system insecure profile
  - Esse comando exibe configurações não seguras da fase de Restrição que o sistema foi projetado para detectar nessa versão do software. A lista de configurações não seguras no perfil é atualizada ao longo do tempo à medida que as práticas recomendadas de segurança continuam a evoluir. Isso não reflete os recursos não confiáveis configurados no momento no dispositivo. É simplesmente uma lista de todas as configurações não seguras da fase de Restrição que o sistema detecta. Consulte os Guias de proteção na seção Recursos adicionais para obter todas as melhores práticas de segurança.

Advertências e considerações

Temporizadores e verificações de configuração não seguras

As verificações de configuração não seguras e as mensagens de aviso detalhadas neste documento são programadas nos temporizadores para limitar a taxa com que frequência eles são executados. Quando uma configuração não segura é corrigida, ela não desaparece imediatamente da saída do comando show system insecure configuration. Há um atraso de até 30 minutos quando o mecanismo de varredura de configuração opera em um ciclo de 30 minutos. Da mesma forma, pode haver um atraso de até dois minutos entre a aplicação de uma configuração não segura e seu syslog %SYS-4-INSECURE_CONFIG correspondente.

Os usuários podem visualizar o tempo restante até a próxima verificação ser executada com o comando show system insecure configuration. O temporizador é exibido na primeira seção de saídas. Este primeiro exemplo mostra que foram feitas alterações na configuração e a próxima verificação de configurações não seguras ocorre em 8 minutos:

<#root>

```
Device#

show system insecure configuration

============================================================
          ACTIVE INSECURE CONFIGURATION DATABASE
============================================================
Generated: Active Configuration Analysis
Total Active Insecure Commands: 1
Database Type: Active (Current State)
Scan Status: Complete
Next Update:

Pending in 8 min 0 sec <<<----------

Database State: Update Scheduled
============================================================
<snip>
```

Este próximo exemplo mostra que nenhuma alteração de configuração foi detectada desde a última varredura, portanto, nenhuma verificação adicional para configurações não seguras é necessária:

<#root>

```
Device#

show system insecure configuration

============================================================
          ACTIVE INSECURE CONFIGURATION DATABASE
============================================================
Generated: Active Configuration Analysis
Total Active Insecure Commands: 1
Database Type: Active (Current State)
Scan Status: Complete
Next Update:

No pending updates <<<----------

Database State: Stable
============================================================
<snip>
```

Os usuários podem forçar uma nova verificação imediata usando o comando test system secure all. Além de solicitar uma nova verificação imediata, este comando exibe a saída do comando show system insecure configuration. Isso é útil para atualizar as configurações sinalizadas como não seguras após uma alteração sem esperar que o temporizador de verificação expire.

Avisos de Configuração Não Segura

Começando em 17.18.2 com a introdução da fase de Aviso, os usuários podem ver esta sintaxe de syslog:

```
%SYS-4-INSECURE_CONFIG: Module: <MODULE> - Command: <COMMAND> - Reason: <REASON> - Remediation: <REMEDI
%SYS-4-INSECURE_DYNAMIC_WARNING: Module: <MODULE> - Command: <COMMAND> - Reason: <REASON> - Remediation
```

Essas mensagens incluem:

- Módulo: O componente que gerou a mensagem de log (como LOGGING, HTTP ou LINE)
- Comando: A configuração específica que disparou a mensagem de aviso
- Razão: O motivo pelo qual esta configuração é sinalizada como não segura
- Correção: Ação necessária para migrar para uma alternativa mais segura

Essas mensagens de aviso não afetam o serviço ou a funcionalidade no dispositivo. A intenção é chamar a atenção para essas configurações não seguras para que possam ser atenuadas de forma proativa pelo usuário.

Note: Começando no Cisco IOS XE versão 26.1.1, as mensagens INSECURE_DYNAMIC_WARNING indicam configurações não seguras na fase de Aviso, enquanto as mensagens INSECURE_CONFIG indicam configurações não seguras na fase de Restrição. Somente as configurações da fase de restrição aparecem na saída do comando show system insecure configuration.

Observe que esses registros são vistos na inicialização ou após a aplicação de uma configuração não segura. Além disso, eles podem reaparecer no dispositivo periodicamente. Você pode encontrar detalhes adicionais sobre essas mensagens e sua sintaxe na Referência de Avisos de Segurança do Cisco IOS XE para Infraestrutura Resiliente.

Exemplo de Syslog visto logo após a configuração

Essas são mensagens de syslog de exemplo vistas logo após a aplicação de uma configuração não segura. Como observado na seção Verificações de Temporizadores e Configuração Insegura, essas mensagens podem levar até dois minutos para serem exibidas após a aplicação da configuração insegura:

```
! Feature in the Warning phase:
    *Jan 1 01:23:45.678: %SYS-4-INSECURE_DYNAMIC_WARNING: Module: HTTP - Command: ip http server - Reas

! Feature in the Restriction phase:
    *Jan 1 01:23:45.678: %SYS-4-INSECURE_CONFIG: Module: FTP - Command: ip ftp source-interface Gigabit
```

Exemplo de Syslog visto na inicialização

Estas são mensagens de exemplo exibidas na inicialização. Uma mensagem é exibida para cada configuração não segura detectada pelo sistema:

```
! Feature in the Warning phase:
    INSECURE DYNAMIC WARNING - Module: HTTP, Command: ip http server , Reason: Legacy protocol poses da

! Feature in the Restriction phase:
    SECURITY WARNING - Module: FTP, Command: ip ftp source-interface GigabitEthernet0/0/0 , Reason: No
```

Modo Inseguro

O Modo Inseguro é apresentado a partir do Cisco IOS XE versão 26.1.1. O Modo Inseguro existe para ajudar a preencher a lacuna entre as implantações atuais e inseguras e as redes futuras e fortalecidas. O acréscimo da configuração do Modo Inseguro permite que os clientes continuem a operar com recursos existentes e não seguros, sinalizando quais configurações representam um risco à segurança e precisam ser minimizadas. Ele também age como uma confirmação de recursos inseguros antes de tentar aplicá-los em um dispositivo padrão de fábrica. O Modo Inseguro também permite o planejamento do Fim da Vida Útil de recursos preteridos antes da Fase Três, na qual eles são completamente removidos. O objetivo do Modo Inseguro é migrar os clientes para redes seguras desde o projeto, minimizando qualquer possível interrupção na funcionalidade.

Para implantações totalmente novas e instalações novas que são padrão de fábrica, o Modo de segurança é definido por padrão (sem modo de sistema inseguro), o que significa que o dispositivo não permite que os usuários apliquem configurações inseguras da fase de Restrição. Os usuários precisam habilitar explicitamente o Modo Inseguro com a configuração global system mode insecure para aplicar os recursos e protocolos inseguros da fase de Restrição. Os recursos

e protocolos não seguros na fase de Aviso ainda podem ser aplicados no Modo de Segurança, mas geram mensagens de aviso.

Verificar Modo de Segurança Atual

Os usuários podem verificar se o dispositivo está no Modo Seguro ou no Modo Inseguro usando o comando show system security mode. O comando show running-config all | include system mode também reflete se o dispositivo está no Modo Seguro ou no Modo Inseguro. A palavra-chave all diz ao dispositivo para incluir configurações padrão na saída, pois o Modo Seguro é a configuração padrão em novas implantações.

Essas saídas refletem um dispositivo no Modo de Segurança:

<#root>

```
Device#

show system security mode


System Security Mode :

Secure



Device#

show running-config all | include system mode



no system mode insecure
```

Os mesmos comandos podem ser usados para verificar se o dispositivo está no modo inseguro:

<#root>

```
Device#

show system security mode


System Security Mode :
```

Insecure

```
Device#
```

show running-config all | include system mode

system mode insecure

Alterar Modo de Segurança

Habilitar Modo Inseguro

Os usuários podem ativar o Modo inseguro com a configuração global system mode insecure:

<#root>

```
Device# configure terminal
Device(config)#
```

system mode insecure

Habilitar Modo Seguro

Os usuários podem ativar o Modo seguro com a configuração global no system mode insecure:

<#root>

```
Device# configure terminal
Device(config)#
```

no system mode insecure

Requisitos para ativar o modo seguro

Para passar para o Modo de Segurança:

- qualquer verificação de configuração não segura deve ser concluída e
- todas as configurações não seguras devem ser removidas do dispositivo

Se a verificação de configuração não segura não for concluída, o sistema solicitará que o usuário tente novamente depois que o temporizador de verificação expirar:

<#root>

```
Device# configure terminal
Device(config)# no system mode insecure
System secure mode cannot be changed to secure as

insecure configuration scanning is in progress. Try after 4 min 0 sec.
```

Os usuários podem forçar uma nova verificação imediata usando o comando test system secure all.

Se, depois que o temporizador expirar e a verificação da configuração estiver concluída, o sistema ainda detectar configurações não seguras, ele não entrará no Modo de Segurança. Essas configurações não seguras devem ser removidas antes que o sistema possa entrar no Modo de Segurança:

<#root>

```
Device(config)# no system mode insecure
System secure mode cannot be changed to secure as

insecure cli(s) are present in system.
```

Quando esses dois requisitos forem atendidos, os usuários poderão ativar o Modo de segurança:

<#root>

```
Device# configure terminal
Device(config)#

no system mode insecure
%SYS-4-SYSTEM_SECURITY_MODE_CHANGE: System Security Mode Changed from INSECURE to SECURE
```

Aplicar configurações não seguras

No Modo Seguro, se um usuário tentar aplicar uma configuração não segura de fase Restrita, uma mensagem de erro será exibida e a configuração não será aplicada. Por exemplo:

<#root>

```
Device# configure terminal
Device(config)# ip ftp source-interface Gi0/0/0


%Error:Insecure configurations are not permitted in secure mode.

 To proceed, set the system mode to insecure using the command

system mode insecure

, and then try again.
Module: FTP, Command: ip ftp source-interface GigabitEthernet0/0/0 , Reason: No encryption is configure

%ERROR: Security policy check failed, configuration can't be applied

Device(config)#end
```

As mensagens exibidas imediatamente após a tentativa de configuração observam que o dispositivo está no Modo de segurança, de modo que as configurações não seguras fornecidas não podem ser aplicadas. Você pode confirmar que as configurações não seguras não foram aplicadas:

```
Device# show running-config | include ip ftp source-interface
Device#
```

Para aplicar configurações não seguras da fase Restriction, os usuários precisam habilitar explicitamente o Modo Inseguro primeiro com a configuração global system mode insecure:

<#root>

```
Device# configure terminal
Device(config)#

system mode insecure


Device(config)# end

Device#show running-config all | include system mode

system mode insecure
```

Quando o dispositivo estiver no modo não seguro, as configurações não seguras da fase de restrição podem ser aplicadas. Uma mensagem de aviso de segurança semelhante é exibida na configuração; no entanto, a configuração não segura é aplicada:

<#root>

```
Device# configure terminal
Device(config)# ip ftp source-interface Gi0/0/0


SECURITY WARNING


 - Module: FTP, Command: ip ftp source-interface GigabitEthernet0/0/0 , Reason: No encryption is config
Device(config)# end
Device# show running-config | include ip ftp source-interface
ip ftp source-interface GigabitEthernet0/0/0
Device#
```

Os usuários também veem uma mensagem de aviso chamando a atenção para a configuração não segura. Devido aos temporizadores enfileirando essas mensagens para limitar a taxa, este syslog pode levar até dois minutos para aparecer após a configuração:

```
%SYS-4-INSECURE_CONFIG: Module: FTP - Command: ip ftp source-interface GigabitEthernet0/0/0 - Reason: N
```

Observe que somente os recursos e protocolos na fase de Restrição exigem ou acionam o Modo inseguro. Os recursos e protocolos que estão na fase de Aviso ainda podem ser aplicados no Modo Seguro

Transição automática para o modo não seguro

Quando um dispositivo Cisco IOS XE é atualizado para 26.1.1 ou posterior, o sistema detecta qualquer configuração insegura da fase de Restrição durante o processo de inicialização e faz automaticamente a transição do dispositivo para o Modo Inseguro. Os usuários não precisam se preocupar com a adição manual da configuração global system mode insecure em si, e não há impacto nos recursos inseguros ao passar para a fase de Restrição.

Este exemplo passa pela transição automática para o Modo Inseguro durante a atualização de 17.18.2 (onde não há contexto do Modo Inseguro) para 26.1.1 (que tem um contexto explícito do Modo Inseguro). O dispositivo começa com a configuração insegura ip ftp source-interface GigabitEthernet0/0/0 aplicada.

Inicialmente, este dispositivo inicia no Cisco IOS XE versão 17.18.2:

```
Device# show version | include Cisco IOS XE Software
Cisco IOS XE Software, Version 17.18.02
```

Foi detectada uma configuração não segura:

<#root>

```
Device# show system insecure configuration
============================================================
          ACTIVE INSECURE CONFIGURATION DATABASE
============================================================
Generated: Active Configuration Analysis

Total Active Insecure Commands: 1 <<<----------

<snip>

+------------------------------------------------------------
| ACTIVE INSECURE CONFIGURATION ENTRY [1/1]
+------------------------------------------------------------
|               Module: FTP
|       Parent Command: NA
|          CLI Command:

ip ftp source-interface GigabitEthernet0/0/0 <<<----------

|          Description: FTP service enabled - transmits credentials and data in plaintext, vulnerable t
|               Reason: No encryption is configured
|          Remediation: Transition to secure file transfer methods using SCP, SFTP, HTTPS protocols
|          Config Mode: configure
|               Status: ACTIVE
|             Severity: HIGH
+------------------------------------------------------------
<snip>

============================================================
                    DATABASE SUMMARY
============================================================
Total Active Entries Processed: 1
<snip>
```

Além disso, não há conceito de Modo seguro ou Modo inseguro nesta versão:

```
Device# show running-config all | include system mode
Device#
```

O dispositivo é então atualizado para 26.1.1, que introduz os Modos Seguro e Inseguro.

```
Device# show version | include Cisco IOS XE Software
Cisco IOS XE Software, Version 26.01.01
```

Ainda há a mesma configuração não segura aplicada:

<#root>

```
Device# show system insecure configuration
============================================================
          ACTIVE INSECURE CONFIGURATION DATABASE
============================================================
Generated: Active Configuration Analysis

Total Active Insecure Commands: 1 <<<----------

<snip>

+------------------------------------------------------------
| ACTIVE INSECURE CONFIGURATION ENTRY [1/1]
+------------------------------------------------------------
|               Module: FTP
|       Parent Command: NA
|          CLI Command:

ip ftp source-interface GigabitEthernet0/0/0 <<<----------

|          Description: FTP service enabled - transmits credentials and data in plaintext, vulnerable t
|               Reason: No encryption is configured
|          Remediation: Transition to secure file transfer methods using SCP, SFTP, HTTPS protocols
|          Config Mode: configure
|               Status: ACTIVE
|             Severity: HIGH
+------------------------------------------------------------
<snip>

============================================================
                    DATABASE SUMMARY
============================================================
Total Active Entries Processed: 1
<snip>
```

Devido à presença desta (ou de qualquer) configuração insegura de fase de restrição, o sistema detecta e faz automaticamente a transição para o Modo Inseguro:

<#root>

```
Device# show system security mode
System Security Mode :
```

```
Insecure
```

E a configuração system mode insecure é aplicada automaticamente:

```
<#root>

Device# show running-config all | include system mode

system mode insecure <<<----------


system mode warning periodicity 24
Device#
```

Observe que a presença de configurações inseguras na fase de Aviso não aciona uma transição para o Modo Inseguro. Somente a presença de configurações inseguras da fase de Restrição aciona a transição automática.

Endurecimento de dispositivos

É altamente recomendável fazer todos os esforços para migrar de recursos e protocolos não seguros para métodos mais seguros antes da fase de Remoção (Fase Três). A Cisco integrou alguns aprimoramentos de facilidade de manutenção para facilitar significativamente a identificação e a correção de configurações inseguras.

Identificar Configurações Não Seguras Aplicadas

Os usuários podem exibir configurações não seguras da fase de Restrição que são aplicadas atualmente com o comando EXEC show system insecure configuration. Esse comando é incluído automaticamente na saída show tech-support nas versões 26.1.1 e posteriores. Este é um exemplo de saída de um dispositivo com três configurações não seguras de fase de restrição aplicadas:

```
<#root>

Device#

show system insecure configuration

============================================================
          ACTIVE INSECURE CONFIGURATION DATABASE
============================================================
```

Generated: Active Configuration Analysis
Total Active Insecure Commands:

3 <<<---------- Number of insecure configurations identified

Database Type: Active (Current State)
Scan Status: Complete
Next Update: Pending in

10 min 0 sec <<<------- Time remaining until this output refreshes to reflect

Database State: Update Scheduled

any configuration changes applied.

==========
SECURE_CONFIG_ACTIVE_INSECURE_CONFIG_DB_WALK: Processing 3 active insecure CLI entries

+----------
| ACTIVE INSECURE CONFIGURATION ENTRY [1/3]
+----------
|

Module

: FTP
| Parent Command: NA
|

CLI Command

: ip ftp source-interface GigabitEthernet0/0/0
|

Description

: FTP service enabled - transmits credentials and data in plaintext, vulnerable to interception
|

Reason

: No encryption is configured
|

Remediation

: Transition to secure file transfer methods using SCP, SFTP, HTTPS protocols
| Config Mode: configure
| Status: ACTIVE
| Severity: HIGH
+----------
SECURE_CONFIG_ACTIVE_INSECURE_CONFIG_DB_WALK: Processed entry 1: ip ftp source-interface GigabitEtherne

```
============================================================
                    DATABASE SUMMARY
============================================================
Total Active Entries Processed: 3
<snip>
```

Essa saída inclui informações importantes sobre o módulo que contém o recurso inseguro, o comando pai ou a configuração, se esta for uma configuração aninhada, o comando CLI específico que foi sinalizado, o motivo pelo qual foi marcado como inseguro e a ação de correção necessária para corrigi-lo.

Os usuários também podem visualizar uma lista abrangente de todos os padrões de CLI não seguros usando o comando show system insecure profile. Enquanto show system insecure configuration mostra configurações não seguras da fase de restrição que estão sendo aplicadas atualmente, show system insecure profile exibe todas as configurações não seguras da fase de restrição que o sistema foi projetado para detectar. A lista de configurações não seguras no perfil é atualizada ao longo do tempo à medida que as práticas recomendadas de segurança continuam a evoluir.

Exemplos de correções para configurações não seguras comuns

Esses exemplos demonstram como os usuários podem detectar, identificar e corrigir várias configurações não seguras comuns. A Cisco implementou software para ajudar a tornar a identificação e a mitigação o mais simples possível, seja os usuários aproveitarem as mensagens do syslog INSECURE_CONFIG ou a saída do comando show system insecure configuration.

Método de transferência de arquivo não seguro

Estas são as mensagens de aviso vistas no dispositivo:

```
%SYS-4-INSECURE_CONFIG: Module: FTP - Command: ip ftp source-interface GigabitEthernet0/0/0 - Reason: N
%SYS-4-INSECURE_CONFIG: Module: FTP - Command: ip ftp username cisco - Reason: No encryption is configu
%SYS-4-INSECURE_CONFIG: Module: FTP - Command: ip ftp password * - Reason: No encryption is configured
```

Você pode executar show system insecure configuration para ver informações adicionais sobre essas configurações não seguras:

<#root>

Device#

show system insecure configuration

```
============================================================
          ACTIVE INSECURE CONFIGURATION DATABASE
============================================================
Generated: Active Configuration Analysis
Total Active Insecure Commands: 3
Database Type: Active (Current State)
Scan Status: Complete
Next Update: No pending updates
Database State: Stable
============================================================
SECURE_CONFIG_ACTIVE_INSECURE_CONFIG_DB_WALK: Processing 3 active insecure CLI entries

+-------------------------------------------------------------
| ACTIVE INSECURE CONFIGURATION ENTRY [1/3]
+-------------------------------------------------------------
|               Module: FTP
|       Parent Command: NA
|          CLI Command:
```

ip ftp source-interface GigabitEthernet0/0/0

```
|          Description: FTP service enabled - transmits credentials and data in plaintext, vulnerable t
|               Reason: No encryption is configured
|          Remediation: Transition to secure file transfer methods using SCP, SFTP, HTTPS protocols
|          Config Mode: configure
|               Status: ACTIVE
|             Severity: HIGH
+-------------------------------------------------------------
SECURE_CONFIG_ACTIVE_INSECURE_CONFIG_DB_WALK: Processed entry 1: ip ftp source-interface GigabitEtherne

+-------------------------------------------------------------
| ACTIVE INSECURE CONFIGURATION ENTRY [2/3]
+-------------------------------------------------------------
|               Module: FTP
|       Parent Command: NA
|          CLI Command:
```

ip ftp username

```
|          Description: FTP service enabled - transmits credentials and data in plaintext, vulnerable t
|               Reason: No encryption is configured
|          Remediation: Transition to secure file transfer methods using SCP, SFTP, HTTPS protocols
|          Config Mode: configure
|               Status: ACTIVE
|             Severity: HIGH
+-------------------------------------------------------------
SECURE_CONFIG_ACTIVE_INSECURE_CONFIG_DB_WALK: Processed entry 2: ip ftp username cisco

+-------------------------------------------------------------
| ACTIVE INSECURE CONFIGURATION ENTRY [3/3]
```

```
+------------------------------------------------------------
|               Module: FTP
|       Parent Command: NA
|          CLI Command:

ip ftp password




|          Description: FTP service enabled - transmits credentials and data in plaintext, vulnerable t
|               Reason: No encryption is configured
|          Remediation: Transition to secure file transfer methods using SCP, SFTP, HTTPS protocols
|          Config Mode: configure
|               Status: ACTIVE
|             Severity: HIGH
+------------------------------------------------------------
SECURE_CONFIG_ACTIVE_INSECURE_CONFIG_DB_WALK: Processed entry 3: ip ftp password cisco

============================================================
                    DATABASE SUMMARY
============================================================
Total Active Entries Processed: 3
<snip>
Device#
```

Esses registros mapeiam diretamente para as seguintes configurações:

```
Device# show running-config | include ip ftp
ip ftp source-interface GigabitEthernet0/0/0
ip ftp username cisco
ip ftp password cisco
```

Os usuários podem reduzir as configurações não seguras com estas alterações:

<#root>

```
Device#

configure terminal


Enter configuration commands, one per line. End with CNTL/Z.
Device# (config)#

no ip ftp source-interface GigabitEthernet0/0/0


Device# (config)#

no ip ftp username
```

```
Device# (config)#

no ip ftp password
```

Protocolos SNMP legados e inseguros

Esta é a mensagem de aviso vista no dispositivo:

```
%SYS-4-INSECURE_CONFIG: Module: SNMP - Command: snmp-server community * ro - Reason: Legacy protocol po
```

Você pode executar show system insecure configuration para ver informações adicionais sobre a configuração insegura:

<#root>

```
Device#

show system insecure configuration


============================================================
          ACTIVE INSECURE CONFIGURATION DATABASE
============================================================
Generated: Active Configuration Analysis
Total Active Insecure Commands: 1
Database Type: Active (Current State)
Scan Status: Complete
Next Update: No pending updates
Database State: Stable
============================================================
SECURE_CONFIG_ACTIVE_INSECURE_CONFIG_DB_WALK: Processing 1 active insecure CLI entries

+------------------------------------------------------------
| ACTIVE INSECURE CONFIGURATION ENTRY [1/1]
+------------------------------------------------------------
|               Module: SNMP
|       Parent Command: NA
|          CLI Command:

snmp-server community
```

```
      RO
```

```
|          Description: SNMP Community string configured - uses insecure SNMPv1/v2c protocol vulnerable
|               Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of e
|          Remediation: Configure SNMP v3 User
|          Config Mode: configure
|               Status: ACTIVE
|              Severity: HIGH
+-------------------------------------------------------------
SECURE_CONFIG_ACTIVE_INSECURE_CONFIG_DB_WALK: Processed entry 1: snmp-server community cisco RO

=============================================================
                    DATABASE SUMMARY
=============================================================
Total Active Entries Processed: 1
<snip>

Device#
```

Estes logs mapeiam diretamente para esta configuração:

<#root>

```
Device# show running-config | include snmp-server

snmp-server community
```

```
      RO
```

Os clientes podem corrigir isso usando SNMPv3 com autenticação e criptografia (authPriv).

Perguntas frequentes

P: Por que a Cisco está fazendo essas alterações?

R: A Cisco está fazendo essas alterações para aprimorar a segurança e a resiliência de sua infraestrutura de rede desativando recursos herdados não seguros, introduzindo proteções e monitoramento mais fortes e simplificando as operações seguras. Esses esforços ajudam a proteger os clientes contra ameaças cibernéticas em evolução, reduzem o tempo de inatividade e preparam as redes para desafios futuros, como a computação quântica. Em geral, a iniciativa tem como objetivo construir uma base moderna, segura e confiável para as tecnologias atuais e futuras

P: O que acontece quando um dispositivo com uma configuração não segura é atualizado para uma versão na fase de Restrição desse recurso?

R: Quando um dispositivo é atualizado para uma versão de Restrição (Fase Dois) para um determinado recurso, o sistema detecta as configurações não seguras durante o processo de inicialização e faz a transição automática do dispositivo para o Modo Inseguro.

P: O que acontece quando um dispositivo com uma configuração não segura é atualizado para uma versão na fase de Remoção desse recurso?

R: Quando um dispositivo é atualizado para uma versão de Remoção (Fase Três) para um determinado recurso, as configurações removidas não estão mais disponíveis. Os usuários devem aderir aos procedimentos de migração padrão para gerenciar comandos obsoletos.

P: Todos os recursos não seguros foram removidos na mesma versão?

R: Nem todos os recursos não seguros são removidos na mesma versão. A Cisco adota uma abordagem em fases para substituir recursos inseguros em três etapas: primeiro, emitir avisos quando recursos inseguros forem configurados ou detectados, depois restringir seu uso desabilitando-os por padrão ou exigindo ação explícita do administrador (através da introdução do Modo inseguro) e, finalmente, remover os recursos inteiramente em versões futuras. Alguns recursos podem ignorar a fase de Restrição e mover diretamente de Avisos para Remoção. O tempo de remoção varia de acordo com o recurso e a plataforma, com os números de versão para avisos, restrições e remoções diferindo entre os sistemas operacionais, como Cisco IOS XE, Cisco IOS XR, Cisco NXOS, Cisco ISE e Cisco ASA/FTD. Esse processo em etapas garante o mínimo de interrupção e permite que os clientes tenham tempo para fazer a transição para alternativas seguras.

P: Quando meu recurso inseguro entra na fase de Restrição ou Remoção?

R: O tempo para quando o recurso inseguro entra na fase de Restrição ou Remoção varia de acordo com o recurso e o sistema operacional. Para obter informações detalhadas, consulte a documentação Detalhes de substituição e remoção de recursos.

P: Quais alternativas existem para o meu recurso inseguro em particular?

R: Os clientes podem consultar a documentação Remoção de recursos e Alternativas sugeridas para identificar alternativas recomendadas para vários recursos e protocolos não seguros.

P: Como posso ver quais configurações não seguras tenho aplicado atualmente?

R: Para ver quais configurações não seguras da fase de Restrição você aplicou no momento, você pode usar o comando show system insecure configuration no Cisco IOS XE 26.1.1 e versões posteriores. Esse comando fornece uma lista abrangente de recursos não seguros da fase de Restrição configurados no dispositivo. Além disso, no Cisco SD-WAN Manager, você pode navegar para Monitor > Advisories e selecionar a guia Insecure Configurations para visualizar configurações não seguras entre dispositivos, grupos de configuração e modelos, com links para etapas de correção. Essa visualização é atualizada aproximadamente a cada 30 minutos para garantir informações atualizadas.

P: Como posso ver uma lista de todas as configurações não seguras possíveis em uma determinada versão de software?

R: Você pode usar o comando show system insecure profile para exibir uma lista completa de todos os padrões CLI inseguros da fase de restrição que o sistema foi projetado para detectar. Ao contrário de show system insecure configuration, que mostra apenas as configurações não seguras aplicadas atualmente, a saída do perfil inclui todas as configurações não seguras conhecidas na fase de Restrição e é atualizada ao longo do tempo à medida que as práticas recomendadas de segurança evoluem.

P: Corrigi uma configuração insegura. Por que ele ainda aparece na saída do comando show system insecure configuration?

R: A verificação de configurações não seguras só é executada periodicamente no modo não seguro. Isso significa que após corrigir uma configuração não segura, o sistema não poderá refletir imediatamente a alteração até que a próxima verificação agendada ocorra, o que acontece em um intervalo de 30 minutos. Esse agendamento garante que os detalhes mais recentes da configuração não segura sejam atualizados e exibidos regularmente, minimizando a sobrecarga necessária para executar a verificação. Você pode usar o comando test system secure all para forçar uma nova verificação imediata para que não seja necessário esperar que o temporizador de verificação expire.

P: Como posso verificar proativamente quais configurações não seguras apliquei antes da atualização?

R: Para verificar proativamente quais configurações não seguras você aplicou antes da

atualização, antes do Cisco IOS XE 17.18.2, os clientes podem usar o Cisco AI Assistant para suporte, disponível na página Cisco Resilient Infrastructure, que permite carregar configurações para identificar recursos não seguros. Uma ferramenta semelhante, o Cisco Config Resilient Infrastructure Tester é outra opção para os clientes. Começando com o Cisco IOS XE 17.18.2 e posterior, os clientes ainda podem usar essas ferramentas, mas você também tem a opção de executar diretamente o comando show system insecure configuration em seus dispositivos para visualizar as configurações não seguras aplicadas atualmente. No entanto, o uso do AI Assistant for Support bot e do Resilient Infrastructure Tester fornece um aumento adicional orientado por IA além do comando CLI direto.

Outros recursos

Os clientes são incentivados a ler esta documentação para complementar a compreensão das melhores práticas de segurança e alternativas para suas configurações atuais e não seguras.

Infraestrutura resiliente da Cisco - Fornece fundamentos essenciais sobre a transição para postura de segurança aprimorada em dispositivos da Cisco e os usuários podem aproveitar o Cisco AI Assistant para Support Bot no canto inferior direito desta página para passar por um fluxo de trabalho guiado para identificar configurações não seguras de várias saídas

Cisco Config Resilient Infrastructure Tester - Uma ferramenta que pode ser usada para verificar configurações não seguras com base em uma configuração atual fornecida

Guia de Fortalecimento do Software Cisco IOS XE - Detalha as melhores práticas para fortalecer seus dispositivos Cisco IOS XE e aumentar a segurança geral de sua rede

Remoção de recursos e alternativas sugeridas - Documenta a lista de recursos e protocolos não seguros que são planejados para eventual remoção, bem como as alternativas recomendadas

Detalhes de substituição e remoção de recursos - Documentos quando recursos e protocolos inseguros específicos entram em fases de aviso e/ou restrição com base na versão do software Cisco IOS XE

Guia de monitoramento e manutenção de SD-WAN - Capítulo de gerenciamento de configuração não segura - Abrange visibilidade centralizada e correção acionável para configurações de recursos não seguros no Cisco Catalyst SD-WAN, ajudando os administradores a identificar e corrigir vulnerabilidades para fortalecer a segurança da rede e manter a conformidade

Infraestrutura resiliente: Referência técnica de Cisco Catalyst SD-WAN e roteamento - Manual de proteção e resiliência de segurança para Cisco Catalyst SD-WAN e roteamento. Ele fornece orientação prescritiva para identificar, corrigir e substituir configurações inseguras em modelos de

gerenciamento baseados em CLI e UI, visando fortalecer a segurança, reduzir a superfície de ataque e proteger os dados, fazendo a transição de alternativas inseguras para seguras e resilientes, garantindo a consistência em todos os modelos operacionais

Cisco C9000 Switching Cisco IOS XE - Manual de Infraestrutura Resiliente - Concentra-se em identificar configurações inseguras e substituí-las por alternativas seguras e resilientes para fortalecer a postura de segurança, reduzir a superfície de ataque e proteger os dados. O manual tem como objetivo garantir a consistência entre os modelos operacionais de CLI e UI, ao mesmo tempo em que aprimora a resiliência da rede e a simplicidade operacional para a família Catalyst 9000

Infraestrutura resiliente sem fio Cisco 9800 - Descreve a estratégia em fases da Cisco para substituir recursos e protocolos inseguros, fornecendo caminhos de migração abrangentes para alternativas seguras para evitar interrupções de serviço durante atualizações de software. Ele inclui tabelas de referência detalhadas para as configurações afetadas no transporte de linha, transferências de arquivos e protocolos de gerenciamento, além de orientações sobre os impactos operacionais potenciais da falha na migração

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.