Comprensión de la infraestructura flexible en los dispositivos IOS XE

Contenido

Introducción

En este documento se describe el enfoque de Cisco sobre la infraestructura flexible, que se basa en la seguridad por defecto y la seguridad por diseño.

Prerequisites

Requirements

Si bien no hay requisitos específicos para este documento, una comprensión básica del software Cisco IOS ® XE es extremadamente útil.

Componentes Utilizados

La información de este documento se aplica a todos los dispositivos que pueden ejecutar el software Cisco IOS XE 17.18.2 y versiones posteriores. Esto incluye routers, switches y WLC Cisco IOS XE.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Objetivo

Nuestro objetivo es reducir significativamente la superficie de ataque a los productos de red de Cisco y minimizar las vulnerabilidades de seguridad mediante la configuración predeterminada segura, la eliminación de tecnologías y funciones antiguas no seguras y la seguridad mejorada del producto.

Puede encontrar más detalles sobre el empuje de Cisco para mejorar la condición de seguridad de la red en la documentación de Infraestructura resiliente, así como en la Guía de endurecimiento del software Cisco IOS XE. Sin embargo, este documento se centra principalmente en los aspectos técnicos y las consideraciones que resultan de la implementación por fases de estos cambios de seguridad vitales.

Enfoque por fases

Para garantizar una superficie de ataque reducida y la adopción de las mejores prácticas de seguridad críticas, a la vez que se minimizan las interrupciones y el esfuerzo para nuestros clientes, Cisco está adoptando un enfoque por fases para eliminar las funciones y los protocolos inseguros. Tenga en cuenta que el escalonamiento de las configuraciones inseguras es

específico de cada función o protocolo. Una función puede permanecer en la fase Advertencia mientras otra función entra en la fase Restricción.

Fase uno: Advertencia

Los usuarios reciben advertencias en la CLI al configurar características clave no seguras. Nuestro objetivo es concienciar sobre estas configuraciones poco seguras para que los clientes puedan comenzar a planificar la migración a opciones más seguras. Cisco recomienda encarecidamente que se aborden inmediatamente los mensajes de advertencia inseguros. Las configuraciones inseguras en la fase de advertencia no se activan ni requieren el modo inseguro.

La versión 17.18.2 de Cisco IOS XE es la primera versión de software que introduce la fase de advertencia para funciones inseguras.

Fase dos: Restricción

Las funciones clave no seguras están desactivadas de forma predeterminada y requieren que el usuario realice una acción explícita para activarlas (mediante la introducción del modo no seguro). Las implementaciones existentes siguen funcionando, pero las nuevas instalaciones requieren la habilitación intencionada de esas configuraciones inseguras. Tenga en cuenta que algunas funciones de las plataformas Cisco IOS XE no pueden tener una fase de restricción: los bucles de retorno pueden

simplemente muestre advertencias para varias versiones antes de la eliminación posterior.

La versión 26.1.1 de Cisco IOS XE es la primera versión de software que introduce la fase Restricción para funciones inseguras.

Fase tres: Retiro

Las funciones obsoletas e inseguras se eliminan por completo. El momento de la eliminación de la función varía en función del impacto en el usuario y de la adopción. Por ejemplo, las funciones ampliamente adoptadas como SNMPv2 se eliminan gradualmente más lentamente que las que se utilizan con menos frecuencia.

La versión 26.2.1 de Cisco IOS XE es la primera versión de software que introduce la fase de eliminación para funciones inseguras.

Comandos clave

Estos comandos son extremadamente útiles a medida que los clientes implementan infraestructuras más resistentes. En este documento se hace referencia a estos comandos.

- show system insecure configuration
    - Este comando se utiliza para mostrar las configuraciones no seguras aplicadas actualmente que se encuentran en la fase Restricción. No muestra las configuraciones inseguras que se encuentran en la fase de advertencia o de eliminación. Este comando también muestra el tiempo restante para el siguiente análisis de configuración insegura (detallado en la sección Temporizadores y análisis de configuración insegura).
- show system security mode
    - Este comando proporciona un breve resultado que muestra si el dispositivo está en modo seguro o en modo inseguro.
- show running-config all | include system mode insecure
    - Este comando muestra la configuración en ejecución (incluidas las configuraciones predeterminadas), filtrada en el modo del sistema mediante palabras clave inseguras. Consulte la sección Cambiar modo de seguridad para obtener más información.
- test system secure all
    - Este comando inmediatamente ejecuta una exploración de configuración insegura y muestra el resultado de show system insecure configuration. Esto resulta útil para actualizar las configuraciones marcadas como no seguras después de un cambio sin esperar a que caduque el temporizador de análisis.
- show system insecure profile
    - Este comando muestra las configuraciones inseguras de la fase de restricción que el sistema está diseñado para detectar en esa versión de software. La lista de configuraciones inseguras del perfil se actualiza con el tiempo a medida que las prácticas recomendadas de seguridad siguen evolucionando. Esto no refleja las características inseguras configuradas actualmente en el dispositivo. Se trata simplemente de una lista de todas las configuraciones inseguras de fase de restricción que el sistema detecta. Consulte las guías de refuerzo en la sección de recursos adicionales para obtener información sobre las prácticas de seguridad recomendadas.

Advertencias y consideraciones

Temporizadores y análisis de configuración inseguros

Las comprobaciones de configuración inseguras y los mensajes de advertencia detallados en este documento se programan en temporizadores para limitar la frecuencia con la que se ejecutan.

Cuando se corrige una configuración insegura, no desaparece inmediatamente del resultado de show system insecure configuration. Se produce un retraso de hasta 30 minutos cuando el analizador de configuración funciona en un ciclo de 30 minutos. Del mismo modo, puede haber un retraso de hasta dos minutos entre la aplicación de una configuración insegura y su correspondiente syslog %SYS-4-INSECURE_CONFIG.

Los usuarios pueden ver el tiempo restante hasta que se ejecute el siguiente análisis con el comando show system insecure configuration. El temporizador se muestra en la primera sección de salidas. Este primer ejemplo muestra que se han realizado cambios en la configuración y que la siguiente búsqueda de configuraciones inseguras se realizará en 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>
```

El siguiente ejemplo muestra que no se han detectado cambios de configuración desde el último análisis, por lo que no se necesitan comprobaciones adicionales para las configuraciones no seguras:

<#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>
```

Los usuarios pueden forzar un nuevo escaneo inmediato usando el comando test system secure all. Además de solicitar un nuevo escaneo inmediato, este comando muestra el resultado de show system insecure configuration. Esto es útil para actualizar las configuraciones marcadas como inseguras después de un cambio sin esperar a que caduque el temporizador de escaneo.

Advertencias de configuración inseguras

A partir de 17.18.2 con la introducción de la fase de advertencia, los usuarios pueden ver esta sintaxis 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
```

Estos mensajes incluyen:

- Módulo: Componente que ha generado el mensaje de registro (como LOGGING, HTTP o LINE)
- Comando: La configuración específica que activó el mensaje de advertencia
- Motivo: La razón por la que esta configuración se marca como insegura
- Solución: Acción necesaria para migrar a una alternativa más segura

Estos mensajes de advertencia no afectan al servicio ni a la funcionalidad del dispositivo. La intención es llamar la atención sobre estas configuraciones inseguras para que el usuario pueda mitigarlas de forma proactiva.

Nota: A partir de la versión 26.1.1 de Cisco IOS XE, los mensajes INSECURE_DYNAMIC_WARNING indican configuraciones inseguras en la fase de advertencia, mientras que los mensajes INSECURE_CONFIG indican configuraciones inseguras en la fase de restricción. Sólo las configuraciones de la fase de restricción aparecen en el resultado de show system insecure configuration.

Tenga en cuenta que estos registros se ven al arrancar o después de aplicar una configuración insegura. Además, pueden volver a aparecer en el dispositivo periódicamente. Puede encontrar detalles adicionales con respecto a estos mensajes y su sintaxis en la Referencia de Advertencias de Seguridad de Cisco IOS XE para Infraestructuras Resilientes.

Syslog de ejemplo visto poco después de la configuración

Estos son ejemplos de mensajes de syslog que se ven poco después de aplicar una configuración insegura. Como se indicó en la sección Temporizadores y análisis de configuración insegura, estos mensajes pueden tardar hasta dos minutos en aparecer después de aplicar la configuración 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
```

Ejemplo de Syslog visto al arrancar

Estos son mensajes de ejemplo que se muestran durante el inicio. Se muestra un mensaje para cada configuración insegura que el sistema detecta:

```
! 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

El modo inseguro se introduce a partir de la versión 26.1.1 de Cisco IOS XE. El modo inseguro existe para ayudar a salvar la distancia entre las implementaciones existentes e inseguras y las redes reforzadas futuras. La incorporación de la configuración de modo inseguro permite a los clientes seguir utilizando las funciones existentes que no son seguras, al tiempo que se marcan las configuraciones que suponen un riesgo para la seguridad y que deben mitigarse. También actúa como un reconocimiento de las funciones inseguras antes de intentar aplicarlas en un dispositivo predeterminado de fábrica. El modo inseguro también permite planificar el fin del ciclo de vida de las funciones obsoletas antes de la fase tres, donde se eliminan por completo. El objetivo del modo inseguro es migrar a los clientes a redes seguras por diseño y, al mismo

tiempo, minimizar las posibles interrupciones en la funcionalidad.

En el caso de las implementaciones nuevas y las instalaciones nuevas predeterminadas de fábrica, el modo seguro se establece de forma predeterminada (no system mode insecure), lo que significa que el dispositivo no permite a los usuarios aplicar configuraciones inseguras en la fase de restricción. Los usuarios necesitan habilitar explícitamente el modo inseguro con el modo del sistema insecure global configuration para aplicar las características y los protocolos inseguros de la fase de restricción. Las funciones y protocolos inseguros de la fase de advertencia se pueden seguir aplicando en el modo seguro, pero generan mensajes de advertencia.

Comprobar el modo de seguridad actual

Los usuarios pueden verificar si el dispositivo está en modo seguro o en modo inseguro mediante el comando show system security mode. show running-config all | include system mode también refleja si el dispositivo está en modo seguro o en modo inseguro. La palabra clave all indica al dispositivo que incluya configuraciones predeterminadas en la salida, ya que el modo seguro es la configuración predeterminada en implementaciones nuevas.

Estas salidas reflejan un dispositivo en modo seguro:

<#root>

```
Device#

show system security mode


System Security Mode :

Secure



Device#

show running-config all | include system mode



no system mode insecure
```

Los mismos comandos se pueden utilizar para verificar si el dispositivo está en modo inseguro:

<#root>

```
Device#

show system security mode


System Security Mode :

Insecure



Device#

show running-config all | include system mode



system mode insecure
```

Cambiar modo de seguridad

Activar modo inseguro

Los usuarios pueden habilitar el modo inseguro con el modo de sistema insecure global configuration:

<#root>

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

system mode insecure
```

Activar el modo seguro

Los usuarios pueden habilitar el modo seguro con la configuración global no insegura del modo del sistema:

<#root>

```
Device# configure terminal
```

```
Device(config)#

no system mode insecure
```

Requisitos para habilitar el modo seguro

Para pasar al modo seguro:

- debe completarse cualquier análisis de configuración insegura, y
- todas las configuraciones inseguras deben eliminarse del dispositivo

Si el análisis de la configuración insegura no está completo, el sistema solicita al usuario que vuelva a intentarlo una vez que haya caducado el temporizador de análisis:

<#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.
```

Los usuarios pueden forzar un nuevo escaneo inmediato usando el comando test system secure all.

Si, después de que caduque el temporizador y la exploración de la configuración se ha completado, el sistema sigue detectando configuraciones inseguras, el sistema no entra en el modo seguro. Estas configuraciones inseguras deben eliminarse antes de que el sistema pueda entrar en el modo seguro:

<#root>

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

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

Una vez cumplidos estos dos requisitos, los usuarios pueden activar el modo seguro:

<#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 configuraciones no seguras

En el modo seguro, si un usuario intenta aplicar una configuración no segura de fase restringida, se muestra un mensaje de error y la configuración no se aplica. Por ejemplo:

<#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
```

Los mensajes que se muestran inmediatamente después del intento de configuración indican que el dispositivo se encuentra en modo seguro, por lo que no se pueden aplicar las configuraciones no seguras proporcionadas. Puede confirmar que no se aplicaron las configuraciones inseguras:

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

Para aplicar las configuraciones inseguras de la fase de restricción, los usuarios necesitan habilitar explícitamente el modo inseguro primero con la configuración global insecure del modo del sistema:

<#root>

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

system mode insecure


Device(config)# end

Device#show running-config all | include system mode

system mode insecure
```

Una vez que el dispositivo está en modo inseguro, se pueden aplicar las configuraciones inseguras de la fase de restricción. Se muestra un mensaje de advertencia de seguridad similar durante la configuración; sin embargo, se aplica la configuración insegura:

<#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#
```

Los usuarios también ven un mensaje de advertencia que llama la atención sobre la configuración insegura. Debido a que los temporizadores ponen en cola estos mensajes para limitar su velocidad, este syslog puede tardar hasta dos minutos en aparecer después de la configuración:

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

Tenga en cuenta que solo las funciones y protocolos de la fase de restricción requieren o activan el modo inseguro. Las funciones y los protocolos que se encuentran en la fase de advertencia se pueden seguir aplicando en el modo seguro

Transición automática al modo no seguro

Cuando un dispositivo Cisco IOS XE se actualiza a la versión 26.1.1 o posterior, el sistema detecta cualquier configuración insegura de fase de restricción durante el proceso de arranque y cambia automáticamente el dispositivo al modo inseguro. Los usuarios no tienen que preocuparse por agregar manualmente el modo de sistema a la configuración global insegura, y las funciones inseguras no tienen ningún impacto al pasar a la fase de restricción.

Este ejemplo recorre la transición automática al modo inseguro durante la actualización de 17.18.2 (donde no hay contexto de modo inseguro) a 26.1.1 (que tiene un contexto explícito de modo inseguro). El dispositivo comienza con la configuración insegura ip ftp source-interface GigabitEthernet0/0/0 aplicada.

Inicialmente, este dispositivo se inicia en la versión 17.18.2 de Cisco IOS XE:

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

Se ha detectado una configuración no 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>
```

Además, no existe el concepto de modo seguro o modo inseguro en esta versión:

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

A continuación, el dispositivo se actualiza a la versión 26.1.1, que introduce los modos seguro e inseguro.

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

Sigue habiendo la misma configuración no 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>
```

Debido a la presencia de esta (o cualquier) configuración insegura de fase de restricción, el sistema detecta y pasa automáticamente al modo inseguro:

<#root>

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

Insecure
```

Y la configuración insegura del modo del sistema se aplica automáticamente:

<#root>

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

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


system mode warning periodicity 24
Device#
```

Tenga en cuenta que la presencia de configuraciones inseguras de fase de advertencia no activa una transición al modo inseguro. Solo la presencia de configuraciones inseguras de fase de restricción activa la transición automática.

Refuerzo de dispositivos

Se recomienda encarecidamente que haga todo lo posible para migrar de características y protocolos inseguros a métodos más seguros antes de la fase de eliminación (fase tres). Cisco ha integrado algunas mejoras en la facilidad de mantenimiento para facilitar considerablemente la identificación de las configuraciones inseguras y su corrección.

Identificación de configuraciones no seguras aplicadas

Los usuarios pueden ver las configuraciones inseguras de la fase de restricción que se aplican actualmente con el comando EXEC show system insecure configuration. Este comando se incluye automáticamente en el resultado de show tech-support en las versiones 26.1.1 y posteriores. Este es un ejemplo de salida de un dispositivo con tres configuraciones inseguras de fase de restricción 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>
```

Este resultado incluye información clave sobre el módulo que contiene la función insegura, el comando primario o la configuración si se trata de una configuración anidada, el comando específico de CLI marcado, la razón por la que se marcó como inseguro y la acción de remediación necesaria para corregirlo.

Los usuarios también pueden ver una lista completa de todos los patrones de CLI inseguros mediante el comando show system insecure profile. Mientras que show system insecure configuration muestra las configuraciones inseguras de la fase de restricción que se aplican actualmente, show system insecure profile muestra todas las configuraciones inseguras de la fase de restricción que el sistema está diseñado para detectar. La lista de configuraciones inseguras del perfil se actualiza con el tiempo a medida que las prácticas recomendadas de seguridad siguen evolucionando.

Remediaciones de ejemplo para configuraciones comunes no seguras

Estos ejemplos muestran cómo los usuarios pueden detectar, identificar y remediar varias configuraciones inseguras con las que se suele tropezar. Cisco ha implementado software para ayudar a que la identificación y la mitigación sean lo más sencillas posible, ya sea que los

usuarios aprovechen los mensajes de syslog INSECURE_CONFIG o el resultado de show system insecure configuration.

Método de transferencia de archivos no seguro

Estos son los mensajes de advertencia que se ven en el 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
```

Puede ejecutar show system insecure configuration para ver información adicional sobre estas configuraciones inseguras:

```
<#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#
```

Estos registros se asignan directamente a estas configuraciones:

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

Los usuarios pueden mitigar las configuraciones inseguras con estos cambios:

<#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 heredados e inseguros

Este es el mensaje de advertencia que se ve en el dispositivo:

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

Puede ejecutar show system insecure configuration para ver información adicional sobre la configuración 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#
```

Estos registros se asignan directamente a esta configuración:

<#root>

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

snmp-server community
```

RO

Los clientes pueden solucionar este problema mediante SNMPv3 con autenticación y cifrado (authPriv).

Preguntas frecuentes

A: ¿Por qué está realizando Cisco estos cambios?

R.: Cisco está realizando estos cambios para mejorar la seguridad y la flexibilidad de su infraestructura de red mediante la desactivación de funciones antiguas e inseguras, la introducción de una supervisión y una protección más robustas y la simplificación de las operaciones seguras. Estos esfuerzos ayudan a proteger a los clientes frente a las amenazas cibernéticas en constante evolución, reducen el tiempo de inactividad y preparan las redes para futuros retos, como la informática cuántica. En general, la iniciativa pretende construir una base moderna, segura y fiable para las tecnologías actuales y futuras

A: ¿Qué sucede cuando un dispositivo con una configuración insegura se actualiza a una versión en la fase Restricción para esa función?

R: Cuando un dispositivo se actualiza a una versión de restricción (fase dos) para una función determinada, el sistema detecta las configuraciones inseguras durante el proceso de arranque y cambia automáticamente el dispositivo al modo inseguro.

A: ¿Qué sucede cuando un dispositivo con una configuración insegura se actualiza a una versión en la fase de eliminación para esa función?

R: Cuando un dispositivo se actualiza a una versión de eliminación (fase tres) para una función determinada, las configuraciones eliminadas ya no están disponibles. Los usuarios deben seguir los procedimientos de migración estándar para administrar comandos obsoletos.

A: ¿Se eliminan todas las funciones inseguras en la misma versión?

R: No todas las funciones inseguras se eliminan en la misma versión. Cisco se adhiere a un enfoque por fases para anular el uso de funciones inseguras en tres fases: primero se emiten

advertencias cuando se configuran o detectan funciones inseguras, después se restringe su uso desactivándolas de forma predeterminada o requiriendo una acción explícita del administrador (mediante la introducción del modo inseguro) y, finalmente, se eliminan las funciones por completo en futuras versiones. Algunas funciones pueden omitir la fase Restricción y pasar directamente de Advertencias a Eliminación. El tiempo de eliminación varía según la función y la plataforma, y los números de versión de advertencias, restricciones y eliminaciones difieren entre los sistemas operativos, como Cisco IOS XE, Cisco IOS XR, Cisco NXOS, Cisco ISE y Cisco ASA/FTD. Este proceso por fases garantiza una interrupción mínima y deja tiempo a los clientes para realizar la transición a alternativas seguras.

A: ¿Cuándo pasa mi función insegura a la fase de restricción o eliminación?

R: El tiempo para cuando su función insegura entra en la fase Restricción o Eliminación varía según la función y el sistema operativo. Para obtener información detallada, consulte la documentación Detalles de eliminación y desaprobación de funciones.

A: ¿Qué alternativas existen para mi función insegura en particular?

R: Los clientes pueden consultar la documentación Eliminación de funciones y alternativas sugeridas para identificar las alternativas recomendadas para varias funciones y protocolos inseguros.

A: ¿Cómo puedo ver qué configuraciones inseguras he aplicado actualmente?

R: Para ver qué configuraciones inseguras de fase de restricción ha aplicado actualmente, puede utilizar el comando show system insecure configuration en Cisco IOS XE 26.1.1 y versiones posteriores. Este comando proporciona una lista completa de las funciones inseguras de la fase de restricción configuradas en el dispositivo. Además, en Cisco SD-WAN Manager, puede navegar hasta Monitor > Advisories y seleccionar la pestaña Insecure Configurations para ver las configuraciones inseguras en los dispositivos, grupos de configuración y plantillas, con links a los pasos de remediación. Esta vista se actualiza aproximadamente cada 30 minutos para garantizar que la información esté actualizada.

A: ¿Cómo puedo ver una lista de todas las posibles configuraciones inseguras en una versión de software determinada?

R: Puede utilizar el comando show system insecure profile para ver una lista completa de todos los patrones de CLI inseguros en la fase de restricción que el sistema está diseñado para detectar. A diferencia de show system insecure configuration, que muestra solo las configuraciones inseguras aplicadas actualmente, el resultado del perfil incluye todas las configuraciones inseguras conocidas en la fase Restricción y se actualiza con el tiempo a medida que evolucionan las prácticas recomendadas de seguridad.

A: He corregido una configuración insegura. ¿Por qué sigue apareciendo en el resultado de show system insecure configuration?

R.: El análisis de configuraciones no seguras sólo se ejecuta periódicamente en el modo no seguro. Esto significa que después de corregir una configuración insegura, el sistema no puede reflejar inmediatamente el cambio hasta que se produzca el siguiente análisis planificado, que tiene lugar en un intervalo de 30 minutos. Esta programación garantiza que los últimos detalles de configuración inseguros se actualicen y se muestren con regularidad, a la vez que se minimiza la sobrecarga necesaria para realizar el análisis. Puede utilizar el comando test system secure all para forzar un nuevo escaneo inmediato, de modo que no tenga que esperar a que caduque el temporizador de escaneo.

A: ¿Cómo puedo comprobar de forma proactiva qué configuraciones inseguras he aplicado antes de actualizar?

R: Para comprobar de forma proactiva qué configuraciones inseguras ha aplicado antes de la actualización, antes de Cisco IOS XE 17.18.2, los clientes pueden utilizar el bot Cisco AI Assistant for Support disponible en la página Cisco Resilient Infrastructure, que permite cargar configuraciones para identificar funciones inseguras. Una herramienta similar, el Cisco Config Resilient Infrastructure Tester, es otra opción para los clientes. A partir de Cisco IOS XE 17.18.2 y versiones posteriores, los clientes pueden seguir utilizando estas herramientas, pero también tiene la opción de ejecutar directamente el comando show system insecure configuration en sus dispositivos para ver las configuraciones inseguras aplicadas actualmente. Sin embargo, el uso de la API Assistant para Support bot y Resilient Infrastructure Tester proporciona un aumento adicional impulsado por la IA más allá del comando directo de la CLI.

Recursos adicionales

Se recomienda a los clientes que lean esta documentación para comprender mejor las prácticas recomendadas y alternativas de seguridad a sus configuraciones existentes poco seguras.

Cisco Resilient Infrastructure: proporciona información básica esencial sobre la transición a una condición de seguridad mejorada en los dispositivos de Cisco. Los usuarios pueden aprovechar Cisco AI Assistant for Support Bot en la esquina inferior derecha de esta página para realizar un flujo de trabajo guiado a fin de identificar configuraciones inseguras a partir de varias salidas

Cisco Config Resilient Infrastructure Tester: herramienta que se puede utilizar para comprobar configuraciones no seguras basadas en una configuración en ejecución proporcionada

Guía de refuerzo del software Cisco IOS XE: detalla las prácticas recomendadas para reforzar los dispositivos Cisco IOS XE y aumentar la seguridad general de la red

Eliminación de características y alternativas sugeridas: documenta la lista de características y protocolos inseguros que se planean para una eventual eliminación, así como las alternativas recomendadas

Detalles de eliminación y desaprobación de funciones: documenta cuándo determinadas funciones y protocolos inseguros entran en las fases de advertencia o restricción basadas en la versión de software Cisco IOS XE

Guía de supervisión y mantenimiento de SD-WAN - Capítulo sobre administración de configuraciones inseguras - Cubre la visibilidad centralizada y la remediación procesable para configuraciones de funciones inseguras en Cisco Catalyst SD-WAN, ayudando a los administradores a identificar y solucionar vulnerabilidades para reforzar la seguridad de la red y mantener el cumplimiento

Infraestructura flexible: Cisco Catalyst SD-WAN and Routing Technical Reference: cuaderno de campaña de resistencia y refuerzo de la seguridad para Cisco Catalyst SD-WAN y routing. Proporciona directrices prescriptivas para identificar, remediar y sustituir configuraciones poco seguras en los modelos de gestión basados en la interfaz de usuario y la CLI, con el objetivo de reforzar la seguridad, reducir la superficie de ataque y proteger los datos mediante la transición de alternativas inseguras a alternativas seguras y resistentes, a la vez que se garantiza la coherencia entre los modelos operativos

Cisco C9000 Switching Cisco IOS XE - Resilient Infrastructure Playbook - Se centra en la identificación de configuraciones inseguras y su sustitución por alternativas seguras y resistentes para reforzar la condición en materia de seguridad, reducir la superficie de ataque y proteger los datos. El objetivo del cuaderno es garantizar la uniformidad entre los modelos operativos de interfaz de usuario y CLI, a la vez que se mejora la resistencia de la red y la simplicidad operativa de la familia Catalyst 9000

Cisco 9800 Wireless Resilient Infrastructure: describe la estrategia por fases de Cisco para desaprobar funciones y protocolos no seguros, proporcionando rutas de migración completas para proteger alternativas que eviten interrupciones del servicio durante las actualizaciones de software. Incluye tablas de referencia detalladas para las configuraciones afectadas a través del transporte de línea, transferencias de archivos y protocolos de gestión, junto con orientación sobre los posibles impactos operativos de no migrar

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).