Comprendere l'infrastruttura resiliente sui dispositivi IOS XE

Sommario

- Introduzione
- Prerequisiti
  - Requisiti
  - Componenti usati
- Obiettivo
- Approccio a fasi
  - Fase 1: Avviso
  - Fase 2: Restrizione
  - Fase 3: Rimozione
- Comandi principali
- Avvertenze e considerazioni
  - Timer e analisi di configurazione non sicure
- Avvisi di configurazione non protetta
  - Esempio di syslog visualizzato subito dopo la configurazione
  - Esempio di syslog visualizzato all'avvio
- Modalità non protetta
  - Verifica modalità di protezione corrente
  - Cambia modalità di protezione
    - Abilita modalità non protetta
    - Abilita modalità protetta
    - Requisiti per abilitare la modalità protetta
  - Applica configurazioni non sicure
- Transizione automatica in modalità non protetta
- Dispositivi di protezione avanzata
  - Individuazione configurazioni non sicure applicate
- Esempi di correzioni per le configurazioni non sicure comuni
  - Metodo di trasferimento file non protetto
  - Protocolli SNMP legacy non sicuri
- Domande frequenti (FAQ)
- Ulteriori risorse

Introduzione

Questo documento descrive l'approccio di Cisco all'infrastruttura resiliente, basata su tecnologie sicure per impostazione predefinita e sicure per progettazione.

Prerequisiti

Requisiti

Anche se non sono previsti requisiti specifici per questo documento, una conoscenza di base del software Cisco IOS ® XE è estremamente utile.

Componenti usati

Le informazioni discusse in questo documento sono valide per tutti i dispositivi con software Cisco IOS XE 17.18.2 e versioni successive. Tra questi sono inclusi router, switch e WLC Cisco IOS XE.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Obiettivo

Il nostro obiettivo è ridurre significativamente la superficie di attacco sui prodotti di rete Cisco e ridurre al minimo le vulnerabilità della sicurezza tramite impostazioni predefinite sicure, la rimozione di tecnologie e funzionalità legacy non sicure e una sicurezza dei prodotti migliorata.

Per ulteriori dettagli sul push a Cisco per migliorare la postura della sicurezza di rete, vedere la documentazione relativa a Resilient Infrastructure e la guida alla protezione avanzata del software Cisco IOS XE. Tuttavia, questo documento si concentra principalmente sugli aspetti tecnici e sulle considerazioni risultanti dall'implementazione graduale di queste modifiche di sicurezza fondamentali.

Approccio a fasi

Per garantire una superficie di attacco ridotta e l'adozione di best practice di sicurezza critiche, riducendo al minimo le interruzioni e gli sforzi per i nostri clienti, Cisco sta adottando un approccio in più fasi per rimuovere le funzionalità e i protocolli non sicuri. Si tenga presente che la definizione di configurazioni non sicure è specifica per ogni funzione o protocollo. Una feature può rimanere nella fase di avvertenza mentre un'altra entra nella fase di restrizione.

Fase 1: Avviso

Gli utenti ricevono avvisi dalla CLI durante la configurazione delle funzioni non sicure principali. Il nostro obiettivo è aumentare la consapevolezza di queste configurazioni non sicure in modo che i clienti possano iniziare a pianificare la migrazione a opzioni più sicure. Cisco consiglia vivamente di risolvere immediatamente qualsiasi messaggio di avviso non sicuro. Le configurazioni non sicure nella fase di avviso non attivano o richiedono la modalità non protetta.

Cisco IOS XE versione 17.18.2 è la prima versione software ad introdurre la fase di avviso per le funzionalità non sicure.

Fase 2: Restrizione

Le funzionalità non sicure con chiave sono disabilitate per impostazione predefinita e richiedono un'azione esplicita dell'utente per abilitarle (tramite l'introduzione della modalità non sicura). Le installazioni esistenti continuano a funzionare, ma le nuove installazioni richiedono l'abilitazione intenzionale di tali configurazioni non sicure. Alcune funzionalità delle piattaforme Cisco IOS XE non possono avere una fase di restrizione: possono

è sufficiente visualizzare avvisi per diverse release prima della successiva rimozione.

Cisco IOS XE versione 26.1.1 è la prima versione software ad introdurre la fase Restriction per le funzionalità non sicure.

Fase 3: Rimozione

Le feature obsolete e non sicure vengono completamente rimosse. I tempi di rimozione delle funzionalità variano a seconda dell'impatto e dell'adozione da parte dell'utente. Ad esempio, le funzionalità ampiamente adottate come SNMPv2 prevedono un ritiro graduale più lento rispetto a quelle meno utilizzate.

Cisco IOS XE versione 26.2.1 è la prima versione software ad introdurre la fase di rimozione per le funzionalità non sicure.

Comandi principali

Questi comandi sono estremamente utili quando i clienti implementano infrastrutture più resilienti. In questo documento viene fatto riferimento a questi comandi.

- mostra configurazione sistema non sicuro
  - Questo comando è usato per visualizzare le configurazioni non sicure attualmente applicate che si trovano nella fase Restriction. Non vengono visualizzate le configurazioni non sicure che si trovano nella fase di avviso o di rimozione. Questo comando visualizza anche il tempo rimanente per la successiva analisi della configurazione non protetta (descritta nella sezione Timer e analisi della configurazione non protetta).
- show system security mode
  - Questo comando fornisce un breve output che mostra se il dispositivo è in modalità protetta o non protetta.
- show running-config all | includi modalità di sistema non protetta
  - Con questo comando viene visualizzata la configurazione in esecuzione (incluse le configurazioni predefinite), filtrata in base alle parole chiave non sicure della modalità di sistema. Per ulteriori informazioni, consultare la sezione Modifica modalità di protezione.
- sistema di test protetto
  - Questo comando esegue immediatamente un'analisi della configurazione non protetta e visualizza l'output show system insecure configuration. Ciò è utile per aggiornare le configurazioni contrassegnate come non sicure dopo una modifica senza attendere la scadenza del timer di digitalizzazione.
- mostra profilo non sicuro del sistema
  - Questo comando visualizza le configurazioni non sicure con fase di restrizione che il sistema è progettato per rilevare su quella versione del software. L'elenco delle configurazioni non sicure nel profilo viene aggiornato nel tempo con l'evoluzione continua delle procedure ottimali per la sicurezza. Ciò non riflette le funzionalità non sicure attualmente configurate sul dispositivo. Si tratta semplicemente di un elenco di tutte le configurazioni non sicure con fase di restrizione rilevate dal sistema. Consultare le Guide alla protezione avanzata nella sezione Ulteriori risorse per tutte le best practice di sicurezza.

Avvertenze e considerazioni

Timer e analisi di configurazione non sicure

I controlli della configurazione non sicura e i messaggi di avviso dettagliati in questo documento sono pianificati sui timer per limitare la frequenza con cui vengono eseguiti. La correzione di una configurazione non protetta non comporta la sua scomparsa immediata dall'output show system insecure configuration. Poiché lo scanner di configurazione funziona in un ciclo di 30 minuti, si verifica un ritardo fino a 30 minuti. Analogamente, tra l'applicazione di una configurazione non protetta e il syslog %SYS-4-INSECURE_CONFIG corrispondente possono intercorrere fino a due

minuti.

Gli utenti possono visualizzare il tempo rimanente all'esecuzione dell'analisi successiva con il comando show system insecure configuration. Il timer viene visualizzato nella prima sezione delle uscite. Nel primo esempio viene mostrato che sono state apportate modifiche alla configurazione e che la prossima analisi per rilevare eventuali configurazioni non sicure viene eseguita in 8 minuti:

<#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>
```

L'esempio seguente mostra che non sono state rilevate modifiche alla configurazione dall'ultima analisi, quindi non sono necessari controlli aggiuntivi per le configurazioni non sicure:

<#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>
```

Gli utenti possono forzare una nuova analisi immediata utilizzando il comando test system secure all. Oltre a richiedere una nuova analisi immediata, questo comando visualizza l'output show system insecure configuration. Questo comando è utile per aggiornare le configurazioni con flag non sicuri dopo una modifica senza attendere la scadenza del timer di analisi.

Avvisi di configurazione non protetta

A partire dalla versione 17.18.2, con l'introduzione della fase Warning, gli utenti possono vedere questa sintassi 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
```

Tali messaggi includono:

- Modulo: Il componente che ha generato il messaggio di log (ad esempio LOGGING, HTTP o LINE)
- Comando: Configurazione specifica che ha attivato il messaggio di avviso
- Motivo: Motivo per cui la configurazione è contrassegnata come non sicura
- Correzione: Necessità di intraprendere un'azione per passare a un'alternativa più sicura

Questi messaggi di avviso non influiscono sul servizio o sulla funzionalità del dispositivo. Lo scopo è quello di attirare l'attenzione su queste configurazioni non sicure in modo che possano essere risolte proattivamente dall'utente.

Nota: A partire da Cisco IOS XE versione 26.1.1, i messaggi INSECURE_DYNAMIC_WARNING indicano configurazioni non sicure nella fase Warning, mentre i messaggi INSECURE_CONFIG indicano configurazioni non sicure nella fase Restriction. Nell'output show system insecure configuration vengono visualizzate solo le configurazioni con fase di restrizione.

I registri vengono visualizzati all'avvio o dopo l'applicazione di una configurazione non protetta. Inoltre, possono essere rivisualizzati periodicamente sul dispositivo. Per ulteriori informazioni su questi messaggi e sulla relativa sintassi, vedere la guida di riferimento degli avvisi di sicurezza di

Cisco IOS XE per l'infrastruttura resiliente.

Esempio di syslog visualizzato subito dopo la configurazione

Questi sono messaggi di syslog di esempio che vengono visualizzati poco dopo l'applicazione di una configurazione non protetta. Come indicato nella sezione Timer e analisi della configurazione non protetta, la visualizzazione di questi messaggi può impiegare fino a due minuti dopo l'applicazione della configurazione non protetta:

```
! 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
```

Esempio di syslog visualizzato all'avvio

Questi sono messaggi di esempio visualizzati all'avvio. Viene visualizzato un messaggio per ogni configurazione non protetta rilevata dal 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
```

Modalità non protetta

La modalità non protetta viene introdotta a partire da Cisco IOS XE versione 26.1.1. La modalità non protetta consente di colmare il divario tra le implementazioni esistenti e non sicure e le reti future con protezione avanzata. L'aggiunta della configurazione in modalità non protetta consente ai clienti di continuare a utilizzare le funzioni non sicure esistenti contrassegnando al contempo le configurazioni che presentano rischi per la sicurezza e che devono essere mitigate. Funge anche da riconoscimento delle funzionalità non sicure prima di tentare di applicarle a un dispositivo predefinito. La modalità non protetta consente inoltre di pianificare la fine del ciclo di vita delle feature obsolete prima della terza fase, in cui sono state completamente rimosse. L'obiettivo della modalità non protetta è quello di migrare i clienti verso reti sicure fin dalla progettazione, riducendo al minimo le possibili interruzioni delle funzionalità.

Per le nuove installazioni e le nuove installazioni predefinite in fabbrica, la modalità protetta è impostata per impostazione predefinita (nessuna modalità di sistema non protetta), ovvero il dispositivo non consente agli utenti di applicare configurazioni non sicure con fase di restrizione. Per applicare funzionalità e protocolli non sicuri in fase di restrizione, gli utenti devono abilitare esplicitamente la modalità non protetta con la configurazione globale non protetta in modalità di sistema. Le funzionalità e i protocolli non sicuri nella fase di avviso possono comunque essere applicati in modalità protetta, ma generano messaggi di avviso.

Verifica modalità di protezione corrente

Gli utenti possono verificare se il dispositivo è in modalità protetta o non protetta utilizzando il comando show system security mode. Il comando show running-config all | include system mode indica anche se il dispositivo è in modalità protetta o non protetta. La parola chiave all indica al dispositivo di includere le configurazioni predefinite nell'output, poiché la modalità protetta è l'impostazione predefinita nelle nuove distribuzioni.

Questi output riflettono un dispositivo in modalità protetta:

<#root>

```
Device#

show system security mode


System Security Mode :

Secure



Device#

show running-config all | include system mode



no system mode insecure
```

Gli stessi comandi possono essere utilizzati per verificare se il dispositivo è in modalità non protetta:

<#root>

```
Device#

show system security mode


System Security Mode :

Insecure



Device#

show running-config all | include system mode



system mode insecure
```

Cambia modalità di protezione

Abilita modalità non protetta

Gli utenti possono abilitare la modalità non protetta con la configurazione globale non protetta della modalità di sistema:

<#root>

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

system mode insecure
```

Abilita modalità protetta

Gli utenti possono abilitare la modalità protetta con la configurazione globale non protetta in modalità di sistema:

<#root>

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

```
no system mode insecure
```

Requisiti per abilitare la modalità protetta

Per passare alla modalità protetta:

- qualsiasi analisi della configurazione non sicura deve essere completata e
- tutte le configurazioni non sicure devono essere rimosse dal dispositivo

Se la scansione con configurazione non protetta non è completa, il sistema chiede all'utente di riprovare dopo la scadenza del timer di scansione:

<#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.
```

Gli utenti possono forzare una nuova analisi immediata utilizzando il comando test system secure all.

Se, dopo la scadenza del timer e la scansione della configurazione è stata completata, il sistema rileva comunque eventuali configurazioni non sicure, il sistema non entra in modalità protetta. Prima che il sistema possa entrare in modalità protetta, è necessario rimuovere le configurazioni non sicure:

<#root>

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

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

Una volta soddisfatti entrambi questi requisiti, gli utenti possono attivare la modalità protetta:

<#root>

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

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

Applica configurazioni non sicure

In modalità protetta, se un utente tenta di applicare una configurazione non protetta con fase limitata, viene visualizzato un messaggio di errore e la configurazione non viene applicata. Ad esempio:

<#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
```

Nei messaggi visualizzati subito dopo il tentativo di configurazione viene segnalato che il dispositivo è in modalità protetta e pertanto le configurazioni non protette fornite non possono essere applicate. È possibile confermare che le configurazioni non sicure non sono state applicate:

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

Per applicare configurazioni non sicure con fase di restrizione, gli utenti devono prima abilitare esplicitamente la modalità non sicura con la configurazione globale non sicura della modalità di sistema:

<#root>

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

system mode insecure


Device(config)# end

Device#show running-config all | include system mode

system mode insecure
```

Quando il dispositivo è in modalità non protetta, è possibile applicare le configurazioni non sicure con fase di restrizione. un messaggio di avviso di sicurezza simile viene visualizzato durante la configurazione; tuttavia, viene applicata la configurazione non sicura:

<#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#
```

Viene inoltre visualizzato un messaggio di avviso che richiama l'attenzione sulla configurazione non protetta. A causa dei timer che accodano questi messaggi per limitarne la velocità, la visualizzazione di questo syslog può impiegare fino a due minuti dopo la configurazione:

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

Solo le funzionalità e i protocolli nella fase Restrizione richiedono o attivano la modalità non protetta. Le funzionalità e i protocolli in fase di avviso possono comunque essere applicati in modalità protetta

Transizione automatica in modalità non protetta

Quando un dispositivo Cisco IOS XE viene aggiornato alla versione 26.1.1 o successive, il sistema rileva eventuali configurazioni non sicure in fase di restrizione durante il processo di avvio e passa automaticamente il dispositivo alla modalità non protetta. Gli utenti non devono preoccuparsi di aggiungere manualmente la configurazione globale non protetta in modalità sistema e non vi è alcun impatto sulle funzionalità non sicure quando passano alla fase Restrizione.

In questo esempio viene esaminata la transizione automatica alla modalità non protetta durante l'aggiornamento da 17.18.2 (in cui non è presente alcun contesto di modalità non protetta) a 26.1.1 (in cui è presente un contesto di modalità non protetta esplicito). Il dispositivo inizia con l'applicazione della configurazione ip ftp source-interface Gigabit Ethernet0/0/0 non sicura.

Inizialmente, il dispositivo viene avviato su Cisco IOS XE versione 17.18.2:

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

È stata rilevata una configurazione non protetta:

<#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>
```

Inoltre, in questa versione non esiste il concetto di modalità protetta o modalità non protetta:

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

Il dispositivo viene quindi aggiornato alla versione 26.1.1, che introduce le modalità protetta e non protetta.

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

È ancora presente la stessa configurazione non sicura applicata:

<#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>
```

A causa della presenza di questa (o di qualsiasi) configurazione non sicura in fase di restrizione, il sistema rileva e passa automaticamente alla modalità non protetta:

<#root>

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

Insecure
```

Inoltre, la configurazione non protetta in modalità sistema viene applicata automaticamente:

<#root>

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

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


system mode warning periodicity 24
Device#
```

La presenza di configurazioni non sicure con fase di avviso non attiva la transizione alla modalità non protetta. Solo la presenza di configurazioni non sicure con fase di restrizione attiva la transizione automatica.

Dispositivi di protezione avanzata

Si consiglia di effettuare tutti gli sforzi necessari per passare da funzionalità e protocolli non sicuri a metodi più sicuri prima della fase di rimozione (fase tre). Cisco ha integrato alcuni miglioramenti nei livelli di servizio per semplificare l'identificazione delle configurazioni non sicure e la relativa correzione.

Individuazione configurazioni non sicure applicate

Gli utenti possono visualizzare le configurazioni non sicure con fase di restrizione applicate con il comando show system insecure configuration EXEC. Questo comando viene incluso automaticamente nell'output show tech-support nelle versioni 26.1.1 e successive. Questo è un esempio di output generato da un dispositivo a cui sono state applicate tre configurazioni non sicure in fase di restrizione:

<#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>
```

Questo output include le informazioni chiave relative al modulo contenente la funzionalità non protetta, il comando o la configurazione padre se si tratta di una configurazione nidificata, il comando CLI specifico contrassegnato, il motivo per cui è stato contrassegnato come non sicuro e l'azione correttiva necessaria per correggerlo.

Gli utenti possono anche visualizzare una lista completa di tutti i modelli CLI non sicuri usando il comando show system insecure profile. Mentre show system insecure configuration mostra le configurazioni non sicure con fase di restrizione attualmente applicate, show system insecure profile visualizza tutte le configurazioni non sicure con fase di restrizione che il sistema è progettato per rilevare. L'elenco delle configurazioni non sicure nel profilo viene aggiornato nel tempo con l'evoluzione continua delle procedure ottimali per la sicurezza.

Esempi di correzioni per le configurazioni non sicure comuni

In questi esempi viene illustrato come gli utenti possono rilevare, identificare e correggere diverse configurazioni non sicure comunemente riscontrate. Cisco ha implementato un software che semplifica al massimo l'identificazione e la mitigazione dei problemi, sia che gli utenti usino i

messaggi syslog INSECURE_CONFIG o l'output show system insecure configuration.

Metodo di trasferimento file non protetto

Di seguito sono riportati i messaggi di avviso visualizzati sul 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
```

È possibile eseguire il comando show system insecure configuration per visualizzare ulteriori informazioni su queste configurazioni non sicure:

```
<#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#
```

Questi log eseguono il mapping direttamente a queste configurazioni:

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

Gli utenti possono ridurre il rischio di configurazioni non sicure con queste modifiche:

```
<#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
```

Protocolli SNMP legacy non sicuri

Questo è il messaggio di avviso visualizzato sul dispositivo:

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

È possibile eseguire il comando show system insecure configuration per visualizzare ulteriori informazioni sulla configurazione non protetta:

```
<#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#
```

Questi log eseguono il mapping direttamente a questa configurazione:

<#root>

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

snmp-server community
```

RO

I clienti possono risolvere questo problema utilizzando il protocollo SNMPv3 con autenticazione e crittografia (authPriv).

Domande frequenti (FAQ)

Q: Perché Cisco sta apportando queste modifiche?

R: Cisco sta apportando queste modifiche per migliorare la sicurezza e la resilienza dell'infrastruttura di rete disabilitando le funzionalità legacy non sicure, introducendo protezione e monitoraggio più avanzati e semplificando le operazioni sicure. Questi sforzi aiutano a proteggere i clienti dall'evoluzione delle minacce informatiche, a ridurre i tempi di inattività e a preparare le reti per le sfide future come l'elaborazione quantistica. In generale, l'iniziativa mira a creare una base moderna, sicura e affidabile per le tecnologie attuali e future

Q: Cosa succede quando un dispositivo con una configurazione non sicura viene aggiornato a una versione nella fase Restriction per tale funzionalità?

A: Quando un dispositivo viene aggiornato a una versione con restrizioni (fase due) per una determinata funzionalità, il sistema rileva le configurazioni non sicure durante il processo di avvio e passa automaticamente il dispositivo alla modalità non protetta.

Q: Cosa succede quando un dispositivo con una configurazione non sicura viene aggiornato a una versione nella fase di rimozione di tale funzionalità?

A: Quando un dispositivo viene aggiornato a una versione di rimozione (fase tre) per una determinata funzionalità, le configurazioni rimosse non sono più disponibili. Gli utenti devono attenersi alle procedure di migrazione standard per la gestione dei comandi obsoleti.

Q: Tutte le funzionalità non sicure sono state rimosse nella stessa release?

R: Non tutte le funzioni non sicure sono state rimosse nella stessa release. Cisco adotta un approccio in tre fasi per eliminare le funzionalità non sicure: emettere prima avvisi quando vengono configurate o rilevate funzionalità non sicure, quindi limitarne l'uso disabilitandole per

impostazione predefinita o richiedendo un'azione esplicita da parte dell'amministratore (tramite l'introduzione della modalità non sicura) e infine rimuovere tutte le funzionalità nelle versioni future. Alcune funzionalità possono ignorare la fase Restriction e passare direttamente da Warnings a Removal. I tempi di rimozione variano a seconda della funzionalità e della piattaforma, con numeri di versione diversi per avvisi, restrizioni e rimozioni nei diversi sistemi operativi, ad esempio Cisco IOS XE, Cisco IOS XR, Cisco NXOS, Cisco ISE e Cisco ASA/FTD. Questo processo in più fasi garantisce un'interruzione minima delle attività e consente ai clienti di passare rapidamente ad alternative sicure.

Q: Quando la funzionalità non protetta passa alla fase Restrizione o Rimozione?

R. I tempi per il passaggio delle funzionalità non sicure alla fase Restrizione o Rimozione variano in base alla funzionalità e al sistema operativo. Per informazioni dettagliate, consultare la documentazione Dettagli rimozione e deprecazione funzionalità.

Q: Quali sono le alternative disponibili per una particolare feature non protetta?

A: Per identificare le alternative consigliate a varie funzioni e protocolli non sicuri, consultare la documentazione sulla rimozione delle funzionalità e sulle alternative suggerite.

Q: Come posso vedere quali configurazioni non sicure ho applicato?

R: Per vedere quali configurazioni non sicure con fase di restrizione sono state applicate, è possibile usare il comando show system insecure configuration su Cisco IOS XE 26.1.1 e versioni successive. Questo comando fornisce un elenco completo delle funzionalità non sicure con fase di restrizione configurate nel dispositivo. Inoltre, in Cisco SD-WAN Manager, è possibile passare a Monitor > Advisories e selezionare la scheda Configurazioni non sicure per visualizzare le configurazioni non sicure tra i dispositivi, i gruppi di configurazione e i modelli, con collegamenti alle fasi di risoluzione dei problemi. Questa visualizzazione viene aggiornata ogni 30 minuti circa per garantire l'aggiornamento delle informazioni.

Q: Come è possibile visualizzare un elenco di tutte le possibili configurazioni non sicure per una determinata versione del software?

A: È possibile usare il comando show system insecure profile per visualizzare un elenco completo di tutti i modelli CLI non sicuri in fase di restrizione che il sistema è progettato per rilevare. A differenza di show system insecure configuration, che mostra solo le configurazioni non sicure attualmente applicate, l'output del profilo include tutte le configurazioni non sicure note nella fase Restrizione e viene aggiornato nel tempo con l'evoluzione delle best practice di sicurezza.

Q: Ho corretto una configurazione non sicura. Perché appare ancora nell'output show system insecure configuration?

R: La ricerca di configurazioni non sicure viene eseguita periodicamente in modalità non protetta. Ciò significa che dopo aver corretto una configurazione non sicura, il sistema non può riflettere immediatamente la modifica fino alla successiva analisi pianificata, che avviene con un intervallo di 30 minuti. Questa pianificazione assicura che i dettagli della configurazione non protetta più recente vengano aggiornati e visualizzati regolarmente, riducendo al minimo il sovraccarico necessario per eseguire la scansione. È possibile utilizzare il comando test system secure all per forzare una nuova analisi immediata in modo da non dover attendere la scadenza del timer di scansione.

Q: Come verificare in modo proattivo quali configurazioni non sicure sono state applicate prima dell'aggiornamento?

R: Per verificare in modo proattivo quali configurazioni non sicure sono state applicate prima dell'aggiornamento, prima di Cisco IOS XE 17.18.2, i clienti possono utilizzare il bot Cisco AI Assistant for Support disponibile nella pagina Cisco Resilient Infrastructure, che consente di caricare le configurazioni per identificare le funzionalità non sicure. Uno strumento simile, il Cisco Config Resilient Infrastructure Tester, è un'altra opzione per i clienti. A partire da Cisco IOS XE 17.18.2 e versioni successive, i clienti possono ancora usare questi strumenti, ma è possibile anche eseguire direttamente il comando show system insecure configuration sui dispositivi per visualizzare le configurazioni non sicure applicate al momento. Tuttavia, l'utilizzo dell'Assistente AI per Support Boot e Resilient Infrastructure Tester offre un'ulteriore espansione basata sull'IA oltre al comando CLI diretto.

Ulteriori risorse

I clienti sono invitati a leggere questa documentazione per integrare la comprensione delle best practice e delle alternative alla sicurezza delle configurazioni esistenti.

Cisco Resilient Infrastructure: fornisce informazioni essenziali sulla transizione verso una postura di sicurezza avanzata sui dispositivi Cisco e gli utenti possono usare Cisco AI Assistant for Support Bot nell'angolo in basso a destra della pagina per eseguire un flusso di lavoro guidato e identificare configurazioni non sicure da vari output

Cisco Config Resilient Infrastructure Tester: strumento che può essere utilizzato per verificare la presenza di configurazioni non sicure in base a una configurazione in esecuzione fornita

Guida alla protezione avanzata del software Cisco IOS XE - Dettagli sulle best practice per rafforzare i dispositivi Cisco IOS XE e aumentare la sicurezza complessiva della rete

Rimozione di funzionalità e alternative suggerite: documenta l'elenco di funzionalità e protocolli non sicuri pianificati per la rimozione finale, nonché le alternative consigliate

Dettagli rimozione e deprecazione funzionalità - Documenta quando specifici protocolli e funzionalità non sicuri entrano nelle fasi di avviso e/o restrizione basate sulla versione del software Cisco IOS XE

Guida alla manutenzione e al monitoraggio di SD-WAN - Capitolo sulla gestione della configurazione non sicura - Copre la visibilità centralizzata e la risoluzione dei problemi praticabili per configurazioni di funzionalità non sicure in Cisco Catalyst SD-WAN, aiutando gli amministratori a identificare e risolvere le vulnerabilità per rafforzare la sicurezza della rete e mantenere la conformità

Infrastruttura resiliente Documentazione tecnica su routing e SD-WAN di Cisco Catalyst - Protezione avanzata e playbook sulla resilienza per Cisco Catalyst SD-WAN e routing. Fornisce una guida prescrittiva per identificare, correggere e sostituire le configurazioni non sicure tra i modelli di gestione basati su interfaccia CLI e UI, allo scopo di rafforzare la sicurezza, ridurre la superficie di attacco e proteggere i dati passando da alternative non sicure a alternative sicure e resilienti, garantendo al contempo la coerenza tra i modelli operativi

Cisco C9000 Switching Cisco IOS XE - Resilient Infrastructure Playbook - Si concentra sull'identificazione delle configurazioni non sicure e sulla loro sostituzione con alternative sicure e resilienti per rafforzare la postura di sicurezza, ridurre la superficie di attacco e proteggere i dati. L'obiettivo del playbook è garantire la coerenza tra i modelli operativi CLI e UI migliorando la resilienza della rete e la semplicità operativa per la famiglia Catalyst 9000

Cisco 9800 Wireless Resilient Infrastructure: illustra la strategia in più fasi adottata da Cisco per eliminare le funzionalità e i protocolli non sicuri, fornendo percorsi di migrazione completi per proteggere le alternative e prevenire interruzioni del servizio durante gli aggiornamenti del software. Include tabelle di riferimento dettagliate per le configurazioni interessate su trasporto di linea, trasferimenti di file e protocolli di gestione, oltre a linee guida sui potenziali impatti operativi della mancata migrazione

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).