Comprendre l'infrastructure résiliente sur les périphériques IOS XE

Table des matières

Introduction

Ce document décrit l'approche de Cisco en matière d'infrastructure résiliente, qui repose sur la sécurisation par défaut et la sécurisation par conception.

Conditions préalables

Exigences

Bien qu'il n'y ait aucune exigence spécifique pour ce document, une compréhension de base de la plate-forme logicielle Cisco IOS ® XE est extrêmement utile.

Composants utilisés

Les informations de ce document s'appliquent à tous les périphériques qui peuvent exécuter le logiciel Cisco IOS XE 17.18.2 et versions ultérieures. Cela inclut les routeurs, commutateurs et WLC Cisco IOS XE.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Objectif

Notre objectif est de réduire de manière significative la surface d'attaque sur les produits réseau Cisco et de minimiser les vulnérabilités de sécurité grâce à des paramètres par défaut sécurisés, la suppression des technologies et fonctionnalités héritées non sécurisées et une sécurité améliorée des produits.

Pour plus d'informations sur la campagne de Cisco visant à améliorer la sécurité du réseau, consultez la documentation relative à l'infrastructure résiliente ainsi que le guide de sécurisation renforcée du logiciel Cisco IOS XE. Cependant, ce document se concentre principalement sur les aspects et les considérations techniques qui résultent de la mise en oeuvre progressive de ces modifications de sécurité essentielles.

Approche progressive

Pour réduire la surface d'attaque et l'adoption des meilleures pratiques en matière de sécurité tout en minimisant les interruptions et les efforts pour nos clients, Cisco adopte une approche progressive pour supprimer les fonctionnalités et les protocoles non sécurisés. Notez que la mise en phase des configurations non sécurisées est spécifique à une fonctionnalité ou à un protocole. Une fonctionnalité peut rester dans la phase d'avertissement tandis qu'une autre fonctionnalité

entre dans la phase de restriction.

Phase 1 : Avertissement

Les utilisateurs reçoivent des avertissements sur la CLI lors de la configuration des principales fonctions non sécurisées. Notre objectif est de sensibiliser les clients à ces configurations non sécurisées afin qu'ils puissent commencer à planifier leur migration vers des options plus sécurisées. Cisco recommande vivement d'adresser immédiatement tout message d'avertissement non sécurisé. Les configurations non sécurisées dans la phase d'avertissement ne déclenchent pas ou ne nécessitent pas le mode non sécurisé.

Cisco IOS XE version 17.18.2 est la première version logicielle à introduire la phase d'avertissement pour les fonctionnalités non sécurisées.

Phase 2 : Restriction

Les principales fonctions non sécurisées sont désactivées par défaut et nécessitent une action explicite de l'utilisateur pour être activées (via l'introduction du mode non sécurisé). Les déploiements existants continuent de fonctionner, mais les nouvelles installations nécessitent l'activation intentionnelle de ces configurations non sécurisées. Notez que certaines fonctionnalités des plates-formes Cisco IOS XE ne peuvent pas avoir de phase de restriction : ils peuvent

il vous suffit d'afficher les avertissements de plusieurs versions avant de les supprimer ultérieurement.

Cisco IOS XE version 26.1.1 est la première version logicielle à introduire la phase de restriction pour les fonctionnalités non sécurisées.

Phase trois : Déménagement

Les fonctions obsolètes et non sécurisées sont entièrement supprimées. Le moment de la suppression des fonctionnalités varie en fonction de l'impact sur l'utilisateur et de l'adoption. Par exemple, les fonctionnalités largement adoptées, telles que SNMPv2, doivent être éliminées progressivement plus lentement que celles qui sont moins couramment utilisées.

Cisco IOS XE version 26.2.1 est la première version logicielle à introduire la phase de suppression des fonctionnalités non sécurisées.

Commandes clés

Ces commandes sont extrêmement utiles lorsque les clients mettent en oeuvre une infrastructure plus résiliente. Ces commandes sont référencées tout au long de ce document.

- show system insecure configuration
    - Cette commande permet d'afficher les configurations non sécurisées actuellement appliquées qui sont en phase de restriction. Il n'affiche pas les configurations non sécurisées en phase d'avertissement ou de suppression. Cette commande affiche également le temps restant pour la prochaine analyse de configuration non sécurisée (détaillée dans la section Minuteurs et analyses de configuration non sécurisées).
- show system security mode
    - Cette commande fournit un bref résultat indiquant si le périphérique est en mode sécurisé ou non sécurisé.
- show running-config all | inclure le mode système non sécurisé
    - Cette commande affiche la configuration en cours (y compris les configurations par défaut), filtrée sur les mots-clés non sécurisés du mode système. Reportez-vous à la section Modifier le mode de sécurité pour plus d'informations.
- test system secure all
    - Cette commande exécute immédiatement une analyse de configuration non sécurisée et affiche le résultat de la commande show system insecure configuration. Cela est utile pour actualiser les configurations avec indicateur de non-sécurité après une modification sans attendre l'expiration du minuteur d'analyse.
- show system insecure profile
    - Cette commande affiche les configurations non sécurisées en phase de restriction que le système est conçu pour détecter sur cette version du logiciel. La liste des configurations non sécurisées dans le profil est mise à jour au fil du temps à mesure que les meilleures pratiques de sécurité évoluent. Cela ne reflète pas les fonctionnalités non sécurisées actuellement configurées sur le périphérique. Il s'agit simplement d'une liste de toutes les configurations non sécurisées en phase de restriction détectées par le système. Reportez-vous aux guides de renforcement dans la section Ressources supplémentaires pour connaître toutes les meilleures pratiques en matière de sécurité.

Mises en garde et considérations

Analyses des minuteurs et des configurations non sécurisées

Les vérifications de configuration non sécurisées et les messages d'avertissement détaillés dans ce document sont planifiés sur des minuteurs afin de limiter la fréquence d'exécution. Lorsqu'une configuration non sécurisée est corrigée, elle ne disparaît pas immédiatement du résultat de la

commande show system insecure configuration. Il y a un délai de 30 minutes lorsque l'analyseur de configuration fonctionne selon un cycle de 30 minutes. De même, il peut y avoir jusqu'à deux minutes de délai entre l'application d'une configuration non sécurisée et son syslog %SYS-4-INSECURE_CONFIG correspondant.

Les utilisateurs peuvent afficher le temps restant jusqu'à l'exécution de la prochaine analyse avec la commande show system insecure configuration. La minuterie est affichée dans la première section des sorties. Ce premier exemple montre que des modifications ont été apportées à la configuration et que la prochaine recherche de configurations non sécurisées a lieu dans 8 minutes :

```
<#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'exemple suivant montre qu'aucune modification de configuration n'a été détectée depuis la dernière analyse. Par conséquent, aucune vérification supplémentaire des configurations non sécurisées n'est nécessaire :

```
<#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>
```

Les utilisateurs peuvent forcer une nouvelle analyse immédiate à l'aide de la commande test system secure all. En plus de demander une nouvelle analyse immédiate, cette commande affiche le résultat de la commande show system insecure configuration. Ceci est utile pour actualiser les configurations avec indicateur de non-sécurité après une modification sans attendre l'expiration du minuteur d'analyse.

Avertissements de configuration non sécurisée

À partir de la version 17.18.2 avec l'introduction de la phase Warning, les utilisateurs peuvent voir la syntaxe syslog suivante :

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

Ces messages incluent :

- Module : Composant qui a généré le message de journal (LOGGING, HTTP ou LINE)
- commande : La configuration spécifique qui a déclenché le message d'avertissement
- Motif : La raison pour laquelle cette configuration est marquée comme non sécurisée
- Correction : Action nécessaire pour migrer vers une alternative plus sécurisée

Ces messages d'avertissement n'ont pas d'impact sur le service ou la fonctionnalité du périphérique. L'objectif est d'attirer l'attention sur ces configurations non sécurisées afin qu'elles puissent être atténuées de manière proactive par l'utilisateur.

Remarque : À partir de la version 26.1.1 de Cisco IOS XE, les messages INSECURE_DYNAMIC_WARNING indiquent des configurations non sécurisées dans la phase Warning tandis que les messages INSECURE_CONFIG indiquent des configurations non sécurisées dans la phase Restriction. Seules les configurations en phase de restriction apparaissent dans le résultat de la commande show system insecure configuration.

Notez que ces journaux sont visibles au démarrage ou après l'application d'une configuration non sécurisée. En outre, ils peuvent réapparaître périodiquement sur le périphérique. Vous trouverez des détails supplémentaires concernant ces messages et leur syntaxe dans le document Resilient Infrastructure Cisco IOS XE Security Warnings Reference.

Exemple de Syslog vu peu après la configuration

Ce sont des exemples de messages syslog vus peu de temps après l'application d'une configuration non sécurisée. Comme indiqué dans la section Analyses des minuteurs et de la configuration non sécurisée, l'affichage de ces messages peut prendre jusqu'à deux minutes après l'application de la configuration non sécurisée :

```
! 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
```

Exemple de Syslog visible au démarrage

Voici des exemples de messages affichés au démarrage. Un message s'affiche pour chaque configuration non sécurisée détectée par le système :

```
! 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
```

Mode non sécurisé

Le mode non sécurisé est introduit à partir de la version 26.1.1 de Cisco IOS XE. Le mode non sécurisé permet de combler l'écart entre les déploiements non sécurisés existants et les futurs réseaux renforcés. L'ajout de la configuration Insecure Mode permet aux clients de continuer à utiliser des fonctionnalités non sécurisées existantes tout en identifiant les configurations qui présentent un risque de sécurité et qui doivent être atténuées. Il sert également d'accusé de réception des fonctionnalités non sécurisées avant d'essayer de les appliquer sur un périphérique par défaut. Le mode non sécurisé permet également de planifier la fin de vie des fonctionnalités déconseillées avant la phase III, où elles sont complètement supprimées. L'objectif du mode non sécurisé est de faire migrer les clients vers des réseaux sécurisés par conception tout en

minimisant les interruptions potentielles de fonctionnement.

Pour les nouveaux déploiements et les nouvelles installations par défaut, le mode sécurisé est défini par défaut (aucun mode système non sécurisé), ce qui signifie que le périphérique ne permet pas aux utilisateurs d'appliquer des configurations non sécurisées en phase de restriction. Les utilisateurs doivent explicitement activer le mode non sécurisé avec la configuration globale du mode système non sécurisé afin d'appliquer les fonctionnalités et les protocoles non sécurisés en phase de restriction. Les fonctions et protocoles non sécurisés de la phase d'avertissement peuvent toujours être appliqués en mode sécurisé, mais ils génèrent des messages d'avertissement.

Vérifier le mode de sécurité actuel

Les utilisateurs peuvent vérifier si le périphérique est en mode sécurisé ou non sécurisé à l'aide de la commande show system security mode. La commande show running-config all | la commande include system mode indique également si le périphérique est en mode sécurisé ou en mode non sécurisé. Le mot clé all indique au périphérique d'inclure les configurations par défaut dans le résultat, car le mode sécurisé est le paramètre par défaut sur les nouveaux déploiements.

Ces résultats reflètent un périphérique en mode sécurisé :

```
<#root>
Device#

show system security mode


System Security Mode :

Secure



Device#

show running-config all | include system mode



no system mode insecure
```

Les mêmes commandes peuvent être utilisées pour vérifier si le périphérique est en mode non

sécurisé :

<#root>

```
Device#

show system security mode


System Security Mode :

Insecure



Device#

show running-config all | include system mode



system mode insecure
```

Modifier le mode de sécurité

Activer le mode non sécurisé

Les utilisateurs peuvent activer le mode non sécurisé avec la configuration globale du mode système non sécurisé :

<#root>

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

system mode insecure
```

Activer le mode sécurisé

Les utilisateurs peuvent activer le mode sécurisé avec la configuration globale no system mode insecure :

<#root>

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

no system mode insecure

Configuration requise pour activer le mode sécurisé

Pour passer en mode sécurisé :

- toute analyse de configuration non sécurisée doit être terminée, et
- toutes les configurations non sécurisées doivent être supprimées du périphérique

Si l'analyse de la configuration non sécurisée n'est pas terminée, le système invite l'utilisateur à réessayer après l'expiration du minuteur d'analyse :

<#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.

Les utilisateurs peuvent forcer une nouvelle analyse immédiate à l'aide de la commande test system secure all.

Si, après l'expiration du minuteur et l'analyse de la configuration, le système détecte toujours des configurations non sécurisées, il ne passe pas en mode sécurisé. Ces configurations non sécurisées doivent être supprimées avant que le système puisse passer en mode sécurisé :

<#root>

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

insecure cli(s) are present in system.

Une fois ces deux conditions remplies, les utilisateurs peuvent activer le mode sécurisé :

<#root>

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

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

Appliquer des configurations non sécurisées

En mode sécurisé, si un utilisateur tente d'appliquer une configuration non sécurisée en phase restreinte, un message d'erreur s'affiche et la configuration n'est pas appliquée. Exemple :

<#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
```

Les messages affichés immédiatement après la tentative de configuration indiquent que le périphérique est en mode sécurisé, de sorte que les configurations non sécurisées fournies ne peuvent pas être appliquées. Vous pouvez confirmer que les configurations non sécurisées n'ont pas été appliquées :

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

Pour appliquer des configurations non sécurisées en phase de restriction, les utilisateurs doivent d'abord activer explicitement le mode non sécurisé avec la configuration globale insecure mode du

système :

<#root>

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

system mode insecure


Device(config)# end

Device#show running-config all | include system mode

system mode insecure
```

Une fois que le périphérique est en mode non sécurisé, les configurations non sécurisées de la phase de restriction peuvent être appliquées. Un message d'avertissement de sécurité similaire s'affiche lors de la configuration ; cependant, la configuration non sécurisée est appliquée :

<#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#
```

Les utilisateurs voient également un message d'avertissement attirant l'attention sur la configuration non sécurisée. En raison des minuteurs qui mettent ces messages en file d'attente afin de les limiter au débit, ce syslog peut prendre jusqu'à deux minutes pour apparaître après la configuration :

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

Notez que seules les fonctionnalités et les protocoles de la phase Restriction nécessitent ou déclenchent le mode non sécurisé. Les fonctionnalités et les protocoles en phase d'avertissement

peuvent toujours être appliqués en mode sécurisé

Transition automatique vers le mode non sécurisé

Lorsqu'un périphérique Cisco IOS XE est mis à niveau vers la version 26.1.1 ou ultérieure, le système détecte toute configuration non sécurisée en phase de restriction au cours du processus de démarrage et fait passer automatiquement le périphérique en mode non sécurisé. Les utilisateurs n'ont pas besoin de se soucier de l'ajout manuel de la configuration globale non sécurisée en mode système, et il n'y a aucun impact sur les fonctionnalités non sécurisées lors du passage à la phase de restriction.

Cet exemple passe en revue la transition automatique vers le mode non sécurisé lors de la mise à niveau de 17.18.2 (où il n'y a pas de contexte de mode non sécurisé) vers 26.1.1 (qui a un contexte de mode non sécurisé explicite). Le périphérique démarre avec la configuration IP ftp source-interface GigabitEthernet0/0/0 non sécurisée appliquée.

Initialement, ce périphérique démarre sur Cisco IOS XE version 17.18.2 :

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

Une configuration non sécurisée a été détectée :

<#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>
```

En outre, il n'existe aucun concept de mode sécurisé ou de mode non sécurisé dans cette version :

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

Le périphérique est ensuite mis à niveau vers la version 26.1.1, qui introduit les modes sécurisé et non sécurisé.

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

La même configuration non sécurisée est toujours appliquée :

<#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>
```

En raison de la présence de cette (ou de toute) configuration non sécurisée en phase de restriction, le système détecte et passe automatiquement en mode non sécurisé :

<#root>

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

Insecure
```

Et la configuration non sécurisée du mode système est appliquée automatiquement :

<#root>

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

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


system mode warning periodicity 24
Device#
```

Veuillez noter que la présence de configurations non sécurisées en phase d'avertissement ne déclenche pas de transition vers le mode non sécurisé. Seule la présence de configurations non sécurisées en phase de restriction déclenche la transition automatique.

Périphériques de durcissement

Nous vous encourageons vivement à tout mettre en oeuvre pour passer de fonctionnalités et de protocoles non sécurisés à des méthodes plus sécurisées avant la phase de suppression (phase trois). Cisco a intégré certaines améliorations en matière de facilité de maintenance pour faciliter considérablement l'identification et la correction des configurations non sécurisées.

Identifier les configurations non sécurisées appliquées

Les utilisateurs peuvent afficher les configurations non sécurisées en phase de restriction qui sont actuellement appliquées avec la commande d'exécution show system insecure configuration. Cette commande est automatiquement incluse dans le résultat de show tech-support dans les versions 26.1.1 et ultérieures. Voici un exemple de sortie d'un périphérique avec trois configurations non sécurisées en phase de restriction appliquées :

```
<#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>
```

Ce résultat inclut des informations clés concernant le module contenant la fonctionnalité non sécurisée, la commande ou la configuration parent s'il s'agit d'une configuration imbriquée, la commande CLI spécifique qui a été marquée comme non sécurisée, la raison pour laquelle elle a été marquée comme non sécurisée et l'action corrective nécessaire pour la corriger.

Les utilisateurs peuvent également afficher une liste complète de tous les modèles CLI non sécurisés à l'aide de la commande show system insecure profile. Tandis que show system insecure configuration affiche les configurations non sécurisées en phase de restriction qui sont actuellement appliquées, show system insecure profile affiche toutes les configurations non sécurisées en phase de restriction que le système est conçu pour détecter. La liste des configurations non sécurisées dans le profil est mise à jour au fil du temps à mesure que les meilleures pratiques de sécurité évoluent.

Exemples de mesures correctives pour les configurations non sécurisées courantes

Ces exemples montrent comment les utilisateurs peuvent détecter, identifier et corriger plusieurs configurations non sécurisées couramment rencontrées. Cisco a mis en oeuvre un logiciel pour faciliter au maximum l'identification et l'atténuation, que les utilisateurs utilisent les messages syslog INSECURE_CONFIG ou le résultat de la commande show system insecure configuration.

Méthode de transfert de fichiers non sécurisée

Voici les messages d'avertissement affichés sur le périphérique :

```
%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
```

Vous pouvez exécuter la commande show system insecure configuration pour afficher des informations supplémentaires sur ces configurations non sécurisées :

<#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#
```

Ces journaux correspondent directement à ces configurations :

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

Les utilisateurs peuvent atténuer les configurations non sécurisées avec ces modifications :

```
<#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
```

Protocoles SNMP hérités et non sécurisés

Voici le message d'avertissement affiché sur le périphérique :

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

Vous pouvez exécuter la commande show system insecure configuration pour afficher des informations supplémentaires sur la configuration non sécurisée :

<#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#
```

Ces journaux correspondent directement à cette configuration :

<#root>

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

snmp-server community

      RO
```

Les clients peuvent y remédier en utilisant SNMPv3 avec authentification et cryptage (authPriv).

Foire aux questions (FAQ)

Q : Pourquoi Cisco apporte-t-il ces modifications ?

R : Cisco apporte ces modifications pour améliorer la sécurité et la résilience de son infrastructure réseau en désactivant les fonctionnalités existantes non sécurisées, en introduisant des protections et une surveillance renforcées et en simplifiant les opérations sécurisées. Ces efforts aident à protéger les clients contre les cybermenaces en constante évolution, à réduire les temps d'arrêt et à préparer les réseaux aux défis futurs comme l'informatique quantique. Dans l'ensemble, l'initiative vise à établir une base moderne, sûre et fiable pour les technologies actuelles et futures

Q : Que se passe-t-il lorsqu'un périphérique dont la configuration n'est pas sécurisée est mis à niveau vers une version en phase de restriction pour cette fonctionnalité ?

A : Lorsqu'un périphérique est mis à niveau vers une version de restriction (phase deux) pour une fonctionnalité donnée, le système détecte les configurations non sécurisées au cours du processus de démarrage et passe automatiquement le périphérique en mode non sécurisé.

Q : Que se passe-t-il lorsqu'un périphérique dont la configuration n'est pas sécurisée est mis à niveau vers une version en phase de suppression pour cette fonctionnalité ?

A : Lorsqu'un périphérique est mis à niveau vers une version de suppression (phase trois) pour

une fonctionnalité donnée, les configurations supprimées ne sont plus disponibles. Les utilisateurs doivent respecter les procédures de migration standard pour gérer les commandes obsolètes.

Q : Toutes les fonctions non sécurisées sont-elles supprimées dans la même version ?

R : Toutes les fonctionnalités non sécurisées ne sont pas supprimées dans la même version. Cisco adopte une approche progressive pour déprécier les fonctionnalités non sécurisées en trois étapes : d'abord émettre des avertissements lorsque des fonctionnalités non sécurisées sont configurées ou détectées, puis restreindre leur utilisation en les désactivant par défaut ou en exigeant une action explicite de l'administrateur (via l'introduction du mode non sécurisé), et enfin supprimer entièrement les fonctionnalités dans les versions futures. Certaines fonctionnalités peuvent ignorer la phase de restriction et passer directement des avertissements à la suppression. Le moment de la suppression varie en fonction de la fonctionnalité et de la plate-forme, les numéros de version des avertissements, restrictions et suppressions différant selon les systèmes d'exploitation tels que Cisco IOS XE, Cisco IOS XR, Cisco NXOS, Cisco ISE et Cisco ASA/FTD. Ce processus par étapes assure une interruption minimale et donne aux clients le temps de passer à des solutions de remplacement sécurisées.

Q : Quand ma fonction non sécurisée passe-t-elle en phase de restriction ou de suppression ?

R : Le moment où votre fonctionnalité non sécurisée passe en phase de restriction ou de suppression varie selon la fonctionnalité et le système d'exploitation. Pour obtenir des informations détaillées, reportez-vous à la documentation Feature Deprecation and Removal Details.

Q : Quelles sont les alternatives possibles pour ma fonction non sécurisée ?

A : Les clients peuvent consulter la documentation Suppression de fonctionnalités et Suggestions de solutions de remplacement pour identifier les alternatives recommandées à diverses fonctionnalités et protocoles non sécurisés.

Q : Comment puis-je voir quelles configurations non sécurisées j'ai actuellement appliquées ?

R : Pour voir quelles configurations non sécurisées en phase de restriction vous avez actuellement appliquées, vous pouvez utiliser la commande show system insecure configuration sur Cisco IOS XE 26.1.1 et versions ultérieures. Cette commande fournit une liste complète des fonctions non sécurisées en phase de restriction configurées sur le périphérique. En outre, dans Cisco SD-WAN Manager, vous pouvez naviguer jusqu'à Monitor > Advisories et sélectionner l'onglet Insecure Configurations pour afficher les configurations non sécurisées entre les périphériques, les groupes de configuration et les modèles, avec des liens vers les étapes de correction. Cet affichage est actualisé environ toutes les 30 minutes pour garantir des informations à jour.

Q : Comment puis-je voir une liste de toutes les configurations non sécurisées possibles sur une version logicielle donnée ?

A : Vous pouvez utiliser la commande show system insecure profile pour afficher une liste complète de tous les modèles CLI non sécurisés en phase de restriction que le système est conçu pour détecter. Contrairement à show system insecure configuration, qui affiche uniquement les configurations non sécurisées actuellement appliquées, le résultat du profil inclut toutes les configurations non sécurisées connues dans la phase de restriction et est mis à jour au fil du temps à mesure que les meilleures pratiques de sécurité évoluent.

Q : J'ai corrigé une configuration non sécurisée. Pourquoi apparaît-il toujours dans le résultat de la commande show system insecure configuration ?

R : L'analyse des configurations non sécurisées ne s'exécute que périodiquement en mode non sécurisé. Cela signifie qu'après avoir corrigé une configuration non sécurisée, le système ne peut pas immédiatement refléter la modification jusqu'à ce que la prochaine analyse programmée ait lieu, ce qui se produit toutes les 30 minutes. Cette planification garantit que les derniers détails de configuration non sécurisés sont mis à jour et affichés régulièrement tout en réduisant la surcharge nécessaire à l'exécution de l'analyse. Vous pouvez utiliser la commande test system secure all pour forcer une nouvelle analyse immédiate afin de ne pas avoir à attendre l'expiration du minuteur d'analyse.

Q : Comment puis-je vérifier de manière proactive quelles configurations non sécurisées j'ai appliquées avant la mise à niveau ?

R : Pour vérifier de manière proactive les configurations non sécurisées que vous avez appliquées avant la mise à niveau, avant Cisco IOS XE 17.18.2, les clients peuvent utiliser le bot Cisco AI Assistant for Support disponible sur la page Cisco Resilient Infrastructure, qui permet de télécharger des configurations pour identifier les fonctionnalités non sécurisées. Un outil similaire, le Cisco Config Resilient Infrastructure Tester est une autre option pour les clients. À partir de Cisco IOS XE 17.18.2 et versions ultérieures, les clients peuvent toujours utiliser ces outils, mais vous avez également la possibilité d'exécuter directement la commande show system insecure configuration sur vos périphériques pour afficher les configurations non sécurisées actuellement appliquées. Cependant, l'utilisation de l'assistant AI pour l'assistance et de Resilient Infrastructure Tester permet d'augmenter les performances de l'IA au-delà de la commande CLI directe.

Ressources supplémentaires

Nous encourageons les clients à lire cette documentation pour mieux comprendre les meilleures pratiques de sécurité et les alternatives à leurs configurations existantes et non sécurisées.

Infrastructure résiliente Cisco - Fournit des informations essentielles sur la transition vers une posture de sécurité améliorée sur les périphériques Cisco. Les utilisateurs peuvent utiliser le Cisco AI Assistant for Support Bot dans le coin inférieur droit de cette page pour suivre un workflow guidé afin d'identifier les configurations non sécurisées à partir de différentes sorties

Cisco Config Resilient Infrastructure Tester : outil permettant de vérifier les configurations non sécurisées en fonction d'une configuration en cours fournie

Guide de sécurisation renforcée du logiciel Cisco IOS XE : décrit les meilleures pratiques pour renforcer vos périphériques Cisco IOS XE et améliorer la sécurité globale de votre réseau

Suppression de fonctionnalités et suggestions de solutions de rechange - Documente la liste des fonctionnalités et protocoles non sécurisés dont la suppression est prévue, ainsi que les solutions de remplacement recommandées

Détails d'élimination et d'élimination des fonctionnalités - Documents lorsque des fonctionnalités et des protocoles non sécurisés spécifiques entrent dans des phases d'avertissement et/ou de restriction basées sur la version du logiciel Cisco IOS XE

Guide de surveillance et de maintenance du SD-WAN - Gestion de la configuration non sécurisée Chapitre - Couvre la visibilité centralisée et la correction exploitable des configurations de fonctions non sécurisées dans le SD-WAN Cisco Catalyst, aidant les administrateurs à identifier et à corriger les vulnérabilités pour renforcer la sécurité du réseau et assurer la conformité

Infrastructure résiliente : Guide de référence technique sur le routage et le SD-WAN de Cisco Catalyst - Durcissement de la sécurité et résilience pour Cisco Catalyst SD-WAN et routage. Il fournit des conseils normatifs pour identifier, corriger et remplacer les configurations non sécurisées sur les modèles de gestion basés sur l'interface de ligne de commande et l'interface utilisateur, dans le but de renforcer la sécurité, de réduire la surface d'attaque et de protéger les données en passant d'alternatives non sécurisées à des alternatives résilientes et sécurisées, tout en assurant la cohérence entre les modèles opérationnels

Commutation Cisco C9000 Cisco IOS XE - Guide de l'infrastructure résiliente - Se concentre sur l'identification des configurations non sécurisées et leur remplacement par des alternatives sécurisées et résilientes pour renforcer la position de sécurité, réduire la surface d'attaque et protéger les données. Le guide vise à assurer la cohérence entre les modèles opérationnels CLI et UI tout en améliorant la résilience du réseau et la simplicité opérationnelle pour la gamme Catalyst 9000

Infrastructure résiliente sans fil Cisco 9800 - Présente la stratégie progressive de Cisco pour déprécier les fonctionnalités et les protocoles non sécurisés, en fournissant des chemins de migration complets vers des alternatives sécurisées afin d'éviter les interruptions de service lors

des mises à niveau logicielles. Il inclut des tables de référence détaillées pour les configurations affectées sur l'ensemble des protocoles de transport de ligne, de transfert de fichiers et de gestion, ainsi que des conseils sur les impacts opérationnels potentiels d'une absence de migration

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.