Inzicht in veerkrachtige infrastructuur op IOS XE-apparaten

Inhoud

Inleiding

In dit document wordt de Cisco-benadering van Resilient Infrastructure beschreven, die is geworteld in secure-by-default en secure-by-design.

Voorwaarden

Vereisten

Hoewel er geen specifieke vereisten zijn voor dit document, is een basiskennis van Cisco IOS ® XE-software uiterst nuttig.

Gebruikte componenten

De informatie in dit document is van toepassing op alle apparaten waarop Cisco IOS XE 17.18.2 en latere software kan worden uitgevoerd. Dit omvat Cisco IOS XE-routers, switches en WLC's.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

doel

Ons doel is om het aanvalsoppervlak van Cisco-netwerkproducten aanzienlijk te verminderen en beveiligingslekken te minimaliseren door middel van veilige standaardinstellingen, verwijdering van onveilige legacy-technologieën en -functies en verbeterde productbeveiliging.

Meer informatie over het streven van Cisco naar verbetering van de netwerkbeveiliging is te vinden in de documentatie over Resilient Infrastructure en in de IOS XE Software Hardening Guide van Cisco. Dit document richt zich echter vooral op de technische aspecten en overwegingen die voortvloeien uit de gefaseerde implementatie van deze essentiële beveiligingswijzigingen.

gefaseerde nadering

Om ervoor te zorgen dat het aanvalsoppervlak kleiner wordt en de beste praktijken voor kritieke beveiliging worden toegepast, terwijl de verstoring en inspanningen voor onze klanten tot een minimum worden beperkt, kiest Cisco voor een gefaseerde aanpak om onveilige functies en protocollen te verwijderen. Houd er rekening mee dat de fasering van onveilige configuraties functie- of protocolspecifiek is. Eén functie kan in de waarschuwingsfase blijven, terwijl een andere functie in de beperkingsfase komt.

Fase 1: Waarschuwing

Gebruikers ontvangen waarschuwingen op de CLI bij het configureren van belangrijke onveilige functies. Ons doel is om het bewustzijn van deze onveilige configuraties te vergroten, zodat klanten kunnen beginnen met het plannen om te migreren naar veiligere opties. Cisco raadt ten zeerste aan om onveilige waarschuwingsberichten onmiddellijk aan te pakken. Onveilige configuraties in de waarschuwingsfase activeren of vereisen geen onveilige modus.

Cisco IOS XE versie 17.18.2 is de eerste softwarerelease die de waarschuwingsfase voor onveilige functies introduceert.

Fase 2: Beperking

Belangrijke onveilige functies zijn standaard uitgeschakeld en vereisen expliciete actie van de gebruiker om deze in te schakelen (door de introductie van de onveilige modus). Bestaande implementaties blijven functioneren, maar nieuwe installaties vereisen opzettelijke activering van deze onveilige configuraties. Houd er rekening mee dat sommige functies op Cisco IOS XE-platforms geen beperkingsfase kunnen hebben: ze kunnen

Geef eenvoudig waarschuwingen weer voor verschillende releases voordat u deze vervolgens verwijdert.

Cisco IOS XE versie 26.1.1 is de eerste softwarerelease die de Restrictiefase introduceert voor onveilige functies.

Fase 3: Verwijderen

Verouderde, onveilige functies worden volledig verwijderd. De timing van het verwijderen van functies varieert, afhankelijk van de impact van de gebruiker en de acceptatie. Bijvoorbeeld, veel gebruikte functies zoals SNMPv2 zijn langzamer uit te faseren dan minder vaak gebruikte.

Cisco IOS XE versie 26.2.1 is de eerste softwarerelease die de verwijderingsfase introduceert voor onveilige functies.

Belangrijkste opdrachten

Deze opdrachten zijn uiterst nuttig omdat klanten een veerkrachtigere infrastructuur implementeren. Deze opdrachten worden in dit document vermeld.

- Onveilige systeemconfiguratie weergeven
    - Deze opdracht wordt gebruikt om de momenteel toegepaste, onveilige configuraties weer te geven die zich in de beperkingsfase bevinden. Er worden geen onveilige configuraties weergegeven die zich in de waarschuwings- of verwijderingsfase bevinden. Met deze opdracht wordt ook de resterende tijd weergegeven voor de volgende onveilige configuratie-scan (gedetailleerd in de sectie Timers en onveilige configuratie-scans).
- Systeembeveiligingsmodus weergeven
    - Deze opdracht geeft een korte uitvoer weer die aangeeft of het apparaat zich in de veilige of onveilige modus bevindt.
- Alle actieve configuraties weergeven | Systeemmodus opnemen is onveilig
    - Deze opdracht geeft de actieve configuratie weer (inclusief standaardconfiguraties), gefilterd op de onveilige trefwoorden in de systeemmodus. Raadpleeg het gedeelte Beveiligingsmodus wijzigen of aanvullende details.
- Testsysteem Beveilig alles
    - Met deze opdracht wordt onmiddellijk een onveilige configuratiescan uitgevoerd en wordt de uitvoer van de onveilige configuratie van het systeem weergegeven. Dit is handig om de onveilige gemarkeerde configuraties na een wijziging te vernieuwen zonder te wachten tot de scantimer is verlopen.
- Systeemonveilig profiel weergeven
    - Met deze opdracht worden onveilige configuraties in de beperkingsfase weergegeven die het systeem op die versie van de software moet detecteren. De lijst met onveilige configuraties in het profiel wordt in de loop van de tijd bijgewerkt naarmate de beste praktijken voor beveiliging zich blijven ontwikkelen. Dit is geen weerspiegeling van de onveilige functies die momenteel op het apparaat zijn geconfigureerd. Het is gewoon een lijst van alle Restrictiefase onveilige configuraties die het systeem detecteert. Raadpleeg de Gidsen voor harden in de sectie Aanvullende bronnen voor alle beste beveiligingspraktijken.

Caveats en overwegingen

Timers en onveilige configuratie scans

De onveilige configuratiecontroles en waarschuwingsberichten die in dit document worden beschreven, zijn gepland op timers om te beoordelen hoe vaak ze worden uitgevoerd. Wanneer een onveilige configuratie wordt gecorrigeerd, verdwijnt deze niet onmiddellijk uit de onveilige uitvoer van het systeem. Er is een vertraging van maximaal 30 minuten omdat de configuratiescanner werkt met een cyclus van 30 minuten. Evenzo kan er een vertraging van maximaal twee minuten zijn tussen het toepassen van een onveilige configuratie en de bijbehorende syslog %SYS-4-INSECURE_CONFIG.

Gebruikers kunnen de resterende tijd bekijken totdat de volgende scan wordt uitgevoerd met de opdracht Onveilige configuratie van systeem tonen. De timer wordt weergegeven in het eerste gedeelte van de uitgangen. Dit eerste voorbeeld laat zien dat er configuratiewijzigingen zijn aangebracht en dat de volgende scan voor onveilige configuraties binnen 8 minuten plaatsvindt:

```
<#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>
```

In dit volgende voorbeeld wordt getoond dat er geen configuratiewijzigingen zijn gedetecteerd sinds de laatste scan, zodat er geen extra controles voor onveilige configuraties nodig zijn:

```
<#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>
```

Gebruikers kunnen een onmiddellijke herscan forceren met behulp van het testsysteem secure all command. Deze opdracht vraagt niet alleen om onmiddellijk opnieuw te scannen, maar geeft ook de onveilige uitvoer van het systeem weer. Dit is handig om de onveilige gemarkeerde configuraties na een wijziging te vernieuwen zonder te wachten tot de scantimer is verlopen.

Waarschuwingen voor onveilige configuratie

Vanaf 17.18.2 met de introductie van de waarschuwingsfase kunnen gebruikers deze syslog-syntaxis zien:

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

Deze berichten omvatten:

- Module: de component die het logbericht heeft gegenereerd (zoals LOGGING, HTTP of LINE)
- Opdracht: de specifieke configuratie die het waarschuwingsbericht heeft geactiveerd
- Reden: de reden waarom deze configuratie als onveilig is gemarkeerd
- Herstel: actie nodig om te migreren naar een veiliger alternatief

Deze waarschuwingsberichten hebben geen invloed op de service of functionaliteit van het apparaat. De bedoeling is om de aandacht te vestigen op deze onveilige configuraties, zodat ze proactief kunnen worden beperkt door de gebruiker.

Opmerking: vanaf Cisco IOS XE versie 26.1.1 wijzen de berichten INSECURE_DYNAMIC_WARNING op onveilige configuraties in de waarschuwingsfase, terwijl de berichten INSECURE_CONFIG op onveilige configuraties in de beperkingsfase wijzen. Alleen Restrictiefase-configuraties worden weergegeven in de weergave van onveilige configuratie-uitvoer van het systeem.

Houd er rekening mee dat deze logs worden weergegeven bij het opstarten of na het toepassen van een onveilige configuratie. Bovendien kunnen ze periodiek op het apparaat verschijnen. Meer informatie over deze berichten en de syntaxis ervan vindt u in de Cisco IOS XE Security Warnings Reference (Naslaggids voor beveiligingswaarschuwingen voor Cisco IOS XE).

Voorbeeld syslog kort na configuratie gezien

Dit zijn bijvoorbeeld syslog-berichten die kort na het toepassen van een onveilige configuratie worden gezien. Zoals vermeld in de sectie Timers en onveilige configuratiescans, kunnen deze berichten tot twee minuten duren voordat ze worden weergegeven na het toepassen van de onveilige configuratie:

```
! 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
```

Voorbeeld syslog gezien bij opstarten

Dit zijn voorbeeldberichten die worden weergegeven bij opstarten. Er wordt een bericht weergegeven voor elke onveilige configuratie die het systeem detecteert:

```
! 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
```

onveilige modus

De onveilige modus wordt geïntroduceerd vanaf Cisco IOS XE versie 26.1.1. De onveilige modus bestaat om de kloof tussen bestaande, onveilige implementaties en toekomstige, geharde netwerken te helpen overbruggen. De toevoeging van de configuratie voor de onveilige modus stelt klanten in staat om te blijven werken met bestaande, onveilige functies en tegelijkertijd te markeren welke configuraties een beveiligingsrisico vormen en moeten worden beperkt. Het fungeert ook als een erkenning van onveilige functies voordat u probeert ze toe te passen op een apparaat dat in de fabriek standaard is. De onveilige modus maakt ook een End-of-Life-planning mogelijk voor verouderde functies vóór fase drie, waar ze volledig worden verwijderd. Het doel van Insecure Mode is om klanten te migreren naar secure-by-design netwerken, terwijl potentiële verstoringen van de functionaliteit worden geminimaliseerd.

Voor gloednieuwe implementaties en nieuwe installaties die standaard in de fabriek worden uitgevoerd, is de veilige modus standaard ingesteld (geen systeemmodus onveilig), wat betekent dat het apparaat gebruikers niet toestaat om onveilige configuraties in de beperkingsfase toe te passen. Gebruikers moeten de onveilige modus expliciet inschakelen met de onveilige globale configuratie van de systeemmodus om onveilige functies en protocollen van de beperkingsfase

toe te passen. Onveilige functies en protocollen in de waarschuwingsfase kunnen nog steeds worden toegepast in de veilige modus, maar ze genereren wel waarschuwingsberichten.

Huidige beveiligingsmodus controleren

Gebruikers kunnen controleren of het apparaat zich in de veilige of onveilige modus bevindt met behulp van de opdracht Systeembeveiligingsmodus weergeven. De opdracht show running-config all | include system mode geeft ook aan of het apparaat zich in Secure Mode of Insecure Mode bevindt. Het trefwoord all vertelt het apparaat om standaardconfiguraties in de uitvoer op te nemen, omdat de veilige modus de standaardinstelling is voor nieuwe implementaties.

Deze uitgangen weerspiegelen een apparaat in de veilige modus:

```
<#root>
Device#

show system security mode


System Security Mode :

Secure



Device#

show running-config all | include system mode



no system mode insecure
```

Dezelfde opdrachten kunnen worden gebruikt om te controleren of het apparaat zich in de onveilige modus bevindt:

```
<#root>
Device#

show system security mode


System Security Mode :
```

```
Insecure
```

```
Device#
```

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

```
system mode insecure
```

Beveiligingsmodus wijzigen

Onveilige modus inschakelen

Gebruikers kunnen de onveilige modus inschakelen met de onveilige globale configuratie van de systeemmodus:

<#root>

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

```
system mode insecure
```

Beveiligde modus inschakelen

Gebruikers kunnen de veilige modus inschakelen zonder systeemmodus en onveilige globale configuratie:

<#root>

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

```
no system mode insecure
```

Vereisten voor het inschakelen van de veilige modus

Zo gaat u naar de veilige modus:

- een onveilige configuratie moet volledig worden gescand, en
- Alle onveilige configuraties moeten van het apparaat worden verwijderd

Als het scannen van de onveilige configuratie niet is voltooid, wordt de gebruiker gevraagd het opnieuw te proberen nadat de scantimer is verlopen:

<#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.
```

Gebruikers kunnen een onmiddellijke herscan forceren met behulp van het testsysteem secure all command.

Als het systeem na het verstrijken van de timer en het scannen van de configuratie nog steeds onveilige configuraties detecteert, gaat het systeem niet over naar de veilige modus. Deze onveilige configuraties moeten worden verwijderd voordat het systeem in de veilige modus kan gaan:

<#root>

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

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

Zodra aan beide vereisten is voldaan, kunnen gebruikers de veilige modus inschakelen:

<#root>

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

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

Onveilige configuraties toepassen

Als een gebruiker in de veilige modus een onveilige configuratie in de beperkte fase probeert toe te passen, wordt een foutbericht weergegeven en wordt de configuratie niet toegepast. Voorbeeld:

```
<#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
```

De berichten die onmiddellijk na de configuratiepoging worden weergegeven, merken op dat het apparaat zich in de veilige modus bevindt, zodat de onveilige configuraties die worden geboden, niet kunnen worden toegepast. U kunt bevestigen dat de onveilige configuraties niet zijn toegepast:

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

Om onveilige configuraties in de beperkingsfase toe te passen, moeten gebruikers eerst expliciet de onveilige modus inschakelen met de onveilige globale configuratie in de systeemmodus:

```
<#root>

Device# configure terminal
Device(config)#

system mode insecure
```

```
Device(config)# end

Device#show running-config all | include system mode

system mode insecure
```

Zodra het apparaat zich in de onveilige modus bevindt, kunnen de onveilige configuraties van de beperkingsfase worden toegepast. Bij de configuratie wordt een vergelijkbaar waarschuwingsbericht weergegeven, maar de onveilige configuratie wordt toegepast:

<#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#
```

Gebruikers zien ook een waarschuwingsbericht waarin de aandacht wordt gevestigd op de onveilige configuratie. Omdat timers deze berichten in de wachtrij plaatsen om ze te beperken, kan het tot twee minuten duren voordat deze syslog na de configuratie wordt weergegeven:

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

Houd er rekening mee dat alleen functies en protocollen in de beperkingsfase de onveilige modus vereisen of activeren. Functies en protocollen die zich in de waarschuwingsfase bevinden, kunnen nog steeds worden toegepast in de veilige modus

Automatische overgang naar onveilige modus

Wanneer een Cisco IOS XE-apparaat wordt opgewaardeerd naar 26.1.1 of hoger, detecteert het systeem tijdens het opstartproces eventuele onveilige configuraties in de beperkingsfase en schakelt het apparaat automatisch over naar de onveilige modus. Gebruikers hoeven zich geen zorgen te maken over het handmatig toevoegen van de systeemmodus en onveilige globale configuratie zelf, en er is geen impact op onveilige functies wanneer ze naar de beperkingsfase

gaan.

Dit voorbeeld loopt door de automatische overgang naar de onveilige modus tijdens de upgrade van 17.18.2 (waar er geen context voor de onveilige modus is) naar 26.1.1 (die een expliciete context voor de onveilige modus heeft). Het apparaat begint met de onveilige ip-ftp-broninterface GigabitEthernet0/0/0-configuratie.

In eerste instantie start dit apparaat op Cisco IOS XE versie 17.18.2:

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

Er is één onveilige configuratie gedetecteerd:

<#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>
```

Bovendien is er geen concept van veilige modus of onveilige modus op deze versie:

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

Het apparaat wordt vervolgens geüpgraded naar 26.1.1, waarmee de veilige en onveilige modi worden geïntroduceerd.

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

Er is nog steeds dezelfde onveilige configuratie toegepast:

<#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>
```

Vanwege de aanwezigheid van deze (of enige) onveilige configuratie in de beperkingsfase detecteert het systeem automatisch de volgende overgangen naar de onveilige modus:

<#root>

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

Insecure
```

En de onveilige configuratie in de systeemmodus wordt automatisch toegepast:

<#root>

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

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


system mode warning periodicity 24
Device#
```

Houd er rekening mee dat de aanwezigheid van onveilige configuraties in de waarschuwingsfase niet leidt tot een overgang naar de onveilige modus. Alleen de aanwezigheid van onveilige configuraties in de beperkingsfase leidt tot de automatische overgang.

hardingsmiddelen

U wordt sterk aangemoedigd om alles in het werk te stellen om te migreren van onveilige functies en protocollen naar veiligere methoden vóór de verwijderingsfase (fase drie). Cisco heeft enkele verbeteringen in de onderhoudsmogelijkheden geïntegreerd om het identificeren van onveilige configuraties en het corrigeren ervan aanzienlijk eenvoudiger te maken.

Onveilige toegepaste configuraties identificeren

Gebruikers kunnen onveilige configuraties in de beperkingsfase bekijken die momenteel worden toegepast met de opdracht Onveilige configuratie EXEC van het systeem weergeven. Deze opdracht wordt automatisch opgenomen in de show-tech-support uitvoer in versies 26.1.1 en hoger. Dit is een voorbeelduitvoer van een apparaat met drie onveilige configuraties in de beperkingsfase:

<#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>
```

Deze uitvoer bevat belangrijke informatie over de module met de onveilige functie, de bovenliggende opdracht of configuratie als dit een geneste configuratie is, de specifieke CLI-opdracht die is gemarkeerd, de reden waarom deze als onveilig is gemarkeerd en de herstelactie die nodig is om deze te corrigeren.

Gebruikers kunnen ook een uitgebreide lijst met alle onveilige CLI-patronen bekijken met behulp van het onveilige profiel van het opdrachtweergavesysteem. Terwijl de onveilige configuratie van het systeem de onveilige configuraties in de beperkingsfase toont die momenteel worden toegepast, toont het onveilige profiel van het systeem alle onveilige configuraties in de beperkingsfase die het systeem moet detecteren. De lijst met onveilige configuraties in het profiel wordt in de loop van de tijd bijgewerkt naarmate de beste praktijken voor beveiliging zich blijven ontwikkelen.

Voorbeeld van oplossingen voor veelvoorkomende onveilige configuraties

Deze voorbeelden laten zien hoe gebruikers verschillende vaak voorkomende onveilige configuraties kunnen detecteren, identificeren en verhelpen. Cisco heeft software geïmplementeerd om identificatie en mitigatie zo eenvoudig mogelijk te maken, of gebruikers nu gebruikmaken van de INSECURE_CONFIG-syslog-berichten of de onveilige uitvoer van de systeemconfiguratie tonen.

Onveilige methode voor bestandsoverdracht

Dit zijn de waarschuwingsberichten op het apparaat:

```
%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
```

U kunt de onveilige configuratie van het systeem uitvoeren om aanvullende informatie over deze onveilige configuraties te bekijken:

<#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#
```

Deze logs worden rechtstreeks toegewezen aan deze configuraties:

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

Gebruikers kunnen de onveilige configuraties beperken met deze wijzigingen:

<#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
```

Onveilige, verouderde SNMP-protocollen

Dit is de waarschuwingsboodschap op het apparaat:

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

U kunt de onveilige configuratie van het systeem uitvoeren om aanvullende informatie over de onveilige configuratie te bekijken:

<#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#
```

Deze logs worden rechtstreeks toegewezen aan deze configuratie:

<#root>

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

snmp-server community

RO

Klanten kunnen dit verhelpen met behulp van SNMPv3 met verificatie en codering (authPriv).

Veelgestelde vragen (FAQ)

V: Waarom voert Cisco deze veranderingen door?

A: Cisco voert deze wijzigingen door om de beveiliging en veerkracht van zijn netwerkinfrastructuur te verbeteren door onveilige legacy-functies uit te schakelen, sterkere beveiligingen en monitoring in te voeren en veilige bewerkingen te vereenvoudigen. Deze inspanningen helpen klanten te beschermen tegen evoluerende cyberdreigingen, verminderen downtime en bereiden netwerken voor op toekomstige uitdagingen zoals quantum computing. Het doel van het initiatief is om een moderne, veilige en betrouwbare basis te leggen voor huidige en toekomstige technologieën

V: Wat gebeurt er wanneer een apparaat met een onveilige configuratie wordt bijgewerkt naar een release in de beperkingsfase voor die functie?

A: Wanneer een apparaat wordt opgewaardeerd naar een Restriction (Phase Two)-release voor een bepaalde functie, detecteert het systeem de onveilige configuraties tijdens het opstartproces en schakelt het apparaat automatisch over naar de Insecure Mode.

V: Wat gebeurt er wanneer een apparaat met een onveilige configuratie wordt bijgewerkt naar een release in de verwijderingsfase voor die functie?

A: Wanneer een apparaat wordt opgewaardeerd naar een Removal (Phase Three) release voor een bepaalde functie, zijn verwijderde configuraties niet langer beschikbaar. Gebruikers moeten zich houden aan de standaardmigratieprocedures voor het beheer van verouderde opdrachten.

V: Worden alle onveilige functies verwijderd in dezelfde release?

A: Niet alle onveilige functies worden in dezelfde release verwijderd. Cisco hanteert een gefaseerde aanpak om onveilige functies in drie fasen af te keuren: eerst waarschuwingen geven wanneer onveilige functies worden geconfigureerd of gedetecteerd, vervolgens het gebruik ervan beperken door ze standaard uit te schakelen of expliciete actie van de beheerder vereisen (door de introductie van de onveilige modus) en tenslotte de functies volledig verwijderen in toekomstige releases. Sommige functies kunnen de beperkingsfase overslaan en direct van Waarschuwingen

naar Verwijdering gaan. De timing van verwijdering verschilt per functie en platform, waarbij releasenummers voor waarschuwingen, beperkingen en verwijderingen verschillen tussen besturingssystemen zoals Cisco IOS XE, Cisco IOS XR, Cisco NXOS, Cisco ISE en Cisco ASA/FTD. Dit gefaseerde proces zorgt voor minimale verstoring en geeft klanten de tijd om over te stappen naar veilige alternatieven.

V: Wanneer wordt mijn onveilige functie verplaatst naar de beperkings- of verwijderingsfase?

A: De timing voor wanneer uw onveilige functie naar de beperkings- of verwijderingsfase gaat, verschilt per functie en besturingssysteem. Raadpleeg de documentatie met details over afschrijving en verwijdering van functies voor gedetailleerde informatie.

V: Welke alternatieven bestaan er voor mijn specifieke onveilige functie?

A: Klanten kunnen de documentatie Functieverwijdering en Voorgestelde alternatieven raadplegen om aanbevolen alternatieven voor verschillende onveilige functies en protocollen te identificeren.

V: Hoe kan ik zien welke onveilige configuraties ik momenteel heb toegepast?

A: Als u wilt zien welke onveilige configuraties in de beperkingsfase u momenteel hebt toegepast, kunt u de opdracht systeemonveilige configuratie weergeven gebruiken op Cisco IOS XE 26.1.1 en latere versies. Deze opdracht bevat een uitgebreide lijst met onveilige functies in de beperkingsfase die op het apparaat zijn geconfigureerd. Bovendien kunt u in Cisco SD-WAN Manager navigeren naar Monitor > Adviezen en het tabblad Onveilige configuraties selecteren om onveilige configuraties op apparaten, configuratiegroepen en sjablonen te bekijken, met koppelingen naar herstelstappen. Deze weergave wordt ongeveer elke 30 minuten vernieuwd om up-to-date informatie te garanderen.

V: Hoe kan ik een lijst zien met alle mogelijke onveilige configuraties op een bepaalde softwareversie?

A: U kunt de opdracht systeemonveilig profiel weergeven gebruiken om een volledige lijst van alle onveilige CLI-patronen in de beperkingsfase te bekijken die het systeem moet detecteren. In tegenstelling tot de onveilige configuratie van het systeem, die alleen de onveilige configuraties toont die momenteel worden toegepast, bevat de profieluitvoer alle bekende onveilige configuraties in de beperkingsfase en wordt deze in de loop van de tijd bijgewerkt naarmate de beste beveiligingspraktijken evolueren.

V: Ik heb een onveilige configuratie gecorrigeerd. Waarom wordt het nog steeds weergegeven in de onveilige configuratie-uitvoer van het systeem?

A: De scan voor onveilige configuraties wordt alleen periodiek uitgevoerd in de onveilige modus. Dit betekent dat na het corrigeren van een onveilige configuratie, het systeem de verandering niet onmiddellijk kan weergeven totdat de volgende geplande scan plaatsvindt, wat gebeurt met een interval van 30 minuten. Deze planning zorgt ervoor dat de nieuwste onveilige configuratiedetails regelmatig worden bijgewerkt en weergegeven, terwijl de overhead die nodig is om de scan uit te voeren, wordt geminimaliseerd. U kunt het testsysteem gebruiken om alle opdrachten te beveiligen om een onmiddellijke herscan te forceren, zodat u niet hoeft te wachten tot de scantimer is verlopen.

V: Hoe kan ik proactief controleren welke onveilige configuraties ik heb toegepast voordat ik een upgrade uitvoerde?

A: Om proactief te controleren welke onveilige configuraties u hebt toegepast voordat u een upgrade uitvoert, voorafgaand aan Cisco IOS XE 17.18.2, kunnen klanten de Cisco AI Assistant for Support-bot gebruiken die beschikbaar is op de pagina Cisco Resilient Infrastructure, waarmee u configuraties kunt uploaden om onveilige functies te identificeren. Een soortgelijke tool, de Cisco Config Resilient Infrastructure Tester is een andere optie voor klanten. Vanaf Cisco IOS XE 17.18.2 en hoger kunnen klanten deze tools nog steeds gebruiken, maar u hebt ook de mogelijkheid om de onveilige configuratie van het systeem op uw apparaten rechtstreeks uit te voeren om de momenteel toegepaste onveilige configuraties te bekijken. Het gebruik van de AI Assistant for Support-bot en Resilient Infrastructure Tester biedt echter extra AI-gestuurde augmentatie naast de directe CLI-opdracht.

Aanvullende bronnen

Klanten worden aangemoedigd om deze documentatie door te lezen om meer inzicht te krijgen in best practices voor beveiliging en alternatieven voor hun bestaande, onveilige configuraties.

Cisco Resilient Infrastructure - Biedt essentiële achtergrondinformatie over de overgang naar een verbeterde beveiligingshouding op Cisco-apparaten en gebruikers kunnen gebruikmaken van de Cisco AI Assistant for Support Bot in de rechterbenedenhoek van deze pagina om door een begeleide workflow te stappen om onveilige configuraties van verschillende uitgangen te identificeren

Cisco Config Resilient Infrastructure Tester - Een tool die kan worden gebruikt om te controleren op onveilige configuraties op basis van een meegeleverde hardloopconfiguratie

Cisco IOS XE Software Hardening Guide - Details best practices om uw Cisco IOS XE-apparaten te verharden en de algehele beveiliging van uw netwerk te verhogen

Verwijdering van functies en voorgestelde alternatieven - Documenten met de lijst van onveilige

functies en protocollen die zijn gepland voor uiteindelijke verwijdering, evenals de aanbevolen alternatieven

Details over afschrijving en verwijdering van functies - Documenten wanneer specifieke onveilige functies en protocollen worden ingevoerd Waarschuwings- en/of beperkingsfasen op basis van de Cisco IOS XE-softwareversie

Gids voor bewaking en onderhoud van SD-WAN - hoofdstuk Onveilig configuratiebeheer - Omvat gecentraliseerde zichtbaarheid en bruikbare oplossingen voor onveilige functieconfiguraties in Cisco Catalyst SD-WAN, zodat beheerders kwetsbaarheden kunnen identificeren en oplossen om de netwerkbeveiliging te versterken en de naleving te handhaven

Veerkrachtige infrastructuur: Cisco Catalyst SD-WAN en Routing Technical Reference - Beveiligingsverharding en veerkracht playbook voor Cisco Catalyst SD-WAN en Routing. Het biedt prescriptieve richtlijnen voor het identificeren, verhelpen en vervangen van onveilige configuraties in CLI- en UI-gebaseerde beheermodellen, met als doel de beveiliging te versterken, het aanvalsoppervlak te verminderen en gegevens te beschermen door over te schakelen van onveilige naar veilige, veerkrachtige alternatieven, terwijl de consistentie tussen operationele modellen wordt gewaarborgd

Cisco C9000 Switching Cisco IOS XE – Resilient Infrastructure Playbook – richt zich op het identificeren van onveilige configuraties en deze te vervangen door veilige, veerkrachtige alternatieven om de beveiligingspositie te versterken, het aanvalsoppervlak te verminderen en gegevens te beschermen. Het draaiboek is bedoeld om consistentie tussen de operationele CLI- en UI-modellen te waarborgen en tegelijkertijd de veerkracht van het netwerk en de operationele eenvoud voor de Catalyst 9000-familie te verbeteren

Cisco 9800 Wireless Resilient Infrastructure - Beschrijft de gefaseerde strategie van Cisco voor het afschrijven van onveilige functies en protocollen en biedt uitgebreide migratiepaden om alternatieven te beveiligen om serviceonderbrekingen tijdens software-upgrades te voorkomen. Het bevat gedetailleerde referentietabellen voor getroffen configuraties voor lijntransport, bestandsoverdracht en beheerprotocollen, samen met richtlijnen voor de potentiële operationele gevolgen van het niet migreren

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.