瞭解IOS XE裝置上的彈性基礎設施

目錄

簡介

本文檔介紹思科的彈性基礎設施方法，該方法植根於預設的安全性和設計的安全性。

必要條件

需求

雖然本檔案沒有特定需求，但深入瞭解Cisco IOS ® XE軟體非常有用。

採用元件

本檔案中的資訊適用於可執行Cisco IOS XE 17.18.2和更新軟體的所有裝置。其中包括Cisco IOS XE路由器、交換機和WLC。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

目標

我們的目標是通過安全預設設定、刪除不安全的傳統技術和功能以及增強產品安全性，有意義地減少思科網路產品的攻擊面，並最大程度地減少安全漏洞。

在彈性基礎架構文檔以及Cisco IOS XE軟體加固指南中，您可以找到有關思科為改善網路安全狀態而推出的更多詳細資訊。但是，本文檔主要側重於分階段實施這些重要安全更改所導致的技術方面和注意事項。

分階段方法

為了確保減少攻擊面，採用關鍵的安全最佳實踐，同時儘量減少對客戶的中斷和工作量，思科採用分階段的方法來消除不安全功能和協定。 請注意，非安全配置的階段特定於功能或協定。 一個功能可以繼續處於「警告」階段，而另一個功能進入「限制」階段。

第一階段：警告

使用者配置主要不安全功能時，會在CLI上收到警告。 我們的目標是提高對不安全配置的認識，以便客戶開始計畫遷移到更安全的選項。 思科強烈建議立即處理所有不安全的警告消息。 在警告階段的不安全配置不會觸發或要求不安全模式。

Cisco IOS XE版本17.18.2是第一個對不安全功能引入警告階段的軟體版本。

第二階段：限制

預設情況下，主要的不安全功能被禁用，需要顯式的使用者操作才能啟用（通過引入不安全模式）。 現有部署仍可繼續運行，但新安裝需要有意啟用這些不安全配置。 請注意，Cisco IOS XE平台上的某些功能不能處於限制階段：他們可以

在後續刪除之前，只需顯示多個版本的警告。

Cisco IOS XE版本26.1.1是第一個針對不安全功能引入限制階段的軟體版本。

第三階段：移除

將完全刪除過時的不安全功能。 功能刪除的時間會因使用者影響及採用情況而異。 例如，廣泛採用的功能（如SNMPv2）的淘汰速度比不常用的功能要慢。

Cisco IOS XE版本26.2.1是第一個針對不安全功能引入刪除階段的軟體版本。

關鍵命令

當客戶實施恢復能力更強的基礎設施時，這些命令非常有用。 本文檔中會引用這些命令。

- show system insecure configuration
  - 此命令用於顯示當前應用的處於限制階段的不安全配置。 它不會顯示處於警告階段或移除階段的不安全配置。 此命令還顯示下一次不安全配置掃描的剩餘時間（在「計時器和不安全配置掃描」部分中進行了詳細說明）。
- show system security mode
  - 此命令提供顯示裝置處於安全模式還是不安全模式的簡要輸出。
- show running-config all | include system mode insecure
  - 此命令顯示運行配置（包括預設配置），按系統模式不安全關鍵字進行過濾。 請參閱更改安全模式部分或其他詳細資訊。
- 測試系統secure all
  - 此命令立即運行不安全配置掃描並顯示show system insecure configuration輸出。 這有助於在更改後刷新不安全標籤的配置，而無需等待掃描計時器過期。
- show system insecure profile
  - 此命令顯示限制階段的不安全配置，系統設計為在該版本的軟體上檢測這些配置。 隨著安全最佳實踐的不斷發展，配置檔案中的不安全配置清單會隨著時間的推移而更新。 這不能反映裝置上當前配置的不安全功能。 它只是系統檢測到的所有限制階段不安全配置的清單。 有關所有最佳安全實踐，請參閱「其他資源」部分中的「加強指南」。

注意事項和注意事項

計時器和不安全配置掃描

本文檔中詳細介紹的不安全的配置檢查和警告消息都安排在計時器上，以限制其運行頻率。 更正不安全配置後，它不會立即從show system insecure configuration輸出中消失。 由於組態掃描器以30分鐘的週期運作，因此延遲高達30分鐘。 同樣，在應用不安全的配置與其對應的%SYS-4-INSECURE_CONFIG系統日誌之間最多可能會出現兩分鐘的延遲。

使用者可以使用show system insecure configuration命令檢視下一次掃描運行之前所剩餘的時間。計時器顯示在輸出的第一部分中。 第一個示例顯示已進行配置更改，並且在8分鐘內對不安全的配置進行下一次掃描：

<#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>
```

下一個示例顯示自上次掃描以來未檢測到任何配置更改，因此不需要對不安全的配置進行其他檢查：

<#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>
```

使用者可以使用test system secure all命令強制立即重新掃描。 除了提示立即重新掃描，此命令還顯示show system insecure configuration輸出。這有助於在更改後刷新不安全標籤的配置，而無需等待掃描計時器過期。

不安全配置警告

從17.18.2引入的「警告」階段開始，使用者可以看到以下系統日誌語法：

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

這些消息包括：

- 模組:生成日誌消息的元件（例如LOGGING、HTTP或LINE）
- 指令:觸發警告消息的特定配置
- 原因:此配置標籤為不安全的原因
- 補救:遷移至更安全的替代方案所需的操作

這些警告消息不會影響裝置上的服務或功能。 其目的是提醒注意這些不安全的配置，以便使用者主動緩解這些配置。

附註：從Cisco IOS XE 26.1.1版開始，INSECURE_DYNAMIC_WARNING消息在警告階段指示不安全的配置，而INSECURE_CONFIG消息在限制階段指示不安全的配置。 show system insecure configuration輸出中僅顯示限制階段配置。

請注意，這些日誌在啟動時或在應用不安全的配置後顯示。 此外，它們可以定期重新出現在裝置上。 有關這些消息及其語法的更多詳細資訊，請參閱彈性基礎設施Cisco IOS XE安全警告參考。

配置後不久出現的系統日誌示例

以下是應用不安全的配置後不久出現的系統日誌消息示例。 如「計時器和不安全配置掃描」部分中所述，應用不安全配置後，可能需要最多兩分鐘時間才會顯示這些消息：

```
! 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
```

啟動時顯示的系統日誌示例

以下是啟動時顯示的示例消息。 系統檢測到的每個不安全配置都會顯示一條消息：

```
! 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
```

不安全模式

從Cisco IOS XE 26.1.1版開始引入不安全模式。 不安全模式有助於彌合現有不安全部署與未來強化網路之間的差距。新增不安全模式配置允許客戶繼續使用現有的不安全功能運行，同時標籤哪些配置會引起安全風險並需要緩解。在嘗試將不安全功能應用到出廠預設裝置之前，它還會充當對不安全功能的確認。 不安全模式還允許在第3階段之前為已棄用的功能進行壽命終止計畫，這些功能將在第三階段被完全刪除。不安全模式的目標是將客戶遷移到基於設計的安全網路，同時儘可能減少任何對功能的潛在中斷。

對於出廠預設的全新部署和全新安裝，預設情況下會設定「安全模式」(no system mode insecure)，這意味著裝置不允許使用者應用限制階段的不安全配置。使用者需要使用系統模式不安全的全域性配置顯式啟用不安全模式，以便應用限制階段不安全功能和協定。 處於警告階段的不安全功能和協定仍可以在安全模式下應用，但它們確實會生成警告消息。

檢查當前安全模式

使用者可以使用show system security mode命令檢查裝置是否處於安全模式或非安全模式。show

running-config all | include system mode命令還反映裝置是處於安全模式還是非安全模式。all關鍵字告訴裝置在輸出中包括預設配置，因為安全模式是新部署的預設設置。

這些輸出反映了處於安全模式的裝置：

```
<#root>
Device#

show system security mode


System Security Mode :

Secure



Device#

show running-config all | include system mode



no system mode insecure
```

可以使用相同的命令檢查裝置是否處於不安全模式：

```
<#root>
Device#

show system security mode


System Security Mode :

Insecure



Device#

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

```
system mode insecure
```

更改安全模式

啟用不安全模式

使用者可以使用系統模式不安全的全域性配置啟用不安全模式：

```
<#root>

Device# configure terminal
Device(config)#

system mode insecure
```

啟用安全模式

使用者可以使用no system mode insecure全域性配置啟用安全模式：

```
<#root>

Device# configure terminal
Device(config)#

no system mode insecure
```

啟用安全模式的要求

若要移至「安全模式」：

- 任何不安全的配置掃描都必須完成，且
- 必須從裝置中刪除所有不安全的配置

如果未完成不安全的配置掃描，則在掃描計時器過期後，系統會提示使用者重試：

```
<#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.
```

使用者可以使用test system secure all命令強制立即重新掃描。

如果在計時器到期且配置掃描完成之後，系統仍然檢測到任何不安全的配置，則系統不會進入安全模式。 必須先刪除這些不安全的配置，然後系統才能進入安全模式：

```
<#root>

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

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

滿足這兩個要求後，使用者可以啟用安全模式：

```
<#root>

Device# configure terminal
Device(config)#

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

應用不安全的配置

在安全模式下，如果使用者嘗試應用受限階段的不安全配置，則會顯示一條錯誤消息，並且不會應用該配置。 舉例來說：

```
<#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
```

配置嘗試後立即顯示的消息表明裝置處於安全模式，因此無法應用提供的不安全配置。 您可以確認未應用不安全的配置：

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

為了應用限制階段不安全配置，使用者需要首先使用系統模式不安全全域性配置顯式啟用不安全模式(Insecure Mode):

```
<#root>

Device# configure terminal
Device(config)#

system mode insecure

Device(config)# end

Device#show running-config all | include system mode

system mode insecure
```

一旦裝置處於不安全模式，即可應用限制階段的不安全配置。 配置時會顯示類似的安全警告消息；但是，應用了不安全的配置：

```
<#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#
```

使用者還會看到一條警告消息，提醒使用者注意不安全的配置。 由於計時器會將這些訊息排隊以限制其速率，因此此系統日誌在設定後最多可能需要兩分鐘才能顯示：

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

請注意，只有處於限制階段的功能和協定需要或觸發不安全模式。 處於警告階段的功能和協定仍可以在安全模式下應用

自動轉換到不安全模式

當Cisco IOS XE裝置升級到26.1.1或更高版本時，系統在引導過程中檢測到任何限制階段的不安全配置，並自動將裝置轉換到不安全模式。使用者無需擔心自己手動新增系統模式不安全全域性配置，而且在進入「限制」階段時，對不安全功能沒有影響。

此範例將介紹從17.18.2（其中沒有不安全模式上下文）升級到26.1.1（具有明確的不安全模式上下文）期間到不安全模式的自動轉換。 裝置從應用的不安全ip ftp source-interface GigabitEthernet0/0/0配置開始。

最初，此裝置在Cisco IOS XE版本17.18.2上啟動：

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

檢測到一個不安全的配置：

<#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>
```

此外，此版本中沒有「安全模式」或「不安全模式」的概念：

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

然後將該裝置升級到26.1.1，這引入了安全模式和不安全模式。

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

仍應用相同的不安全配置：

<#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>
```

由於存在此（或任何）限制階段的不安全配置，系統將檢測並自動轉換到不安全模式：

```
<#root>

Device# show system security mode
System Security Mode :

Insecure
```

系統模式的不安全配置會自動應用：

```
<#root>

Device# show running-config all | include system mode

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


system mode warning periodicity 24
Device#
```

請注意，如果存在「警告 — 階段」不安全配置，則不會觸發向「不安全模式」的轉換。 只有限制

階段的不安全配置才會觸發自動轉換。

加固裝置

強烈建議您盡一切努力，在刪除階段（第三階段）之前，從不安全的功能和協定遷移到更安全的方法。 思科整合了一些可維護性增強功能，使識別不安全配置並對其進行更正變得非常簡單。

確定應用的不安全配置

使用者可以檢視當前使用show system insecure configuration EXEC命令應用的Restriction-phase insecure配置。 此命令在26.1及更新版本中自動包含在show tech-support輸出中。 以下是應用了三個限制階段不安全配置的裝置的輸出示例：

```
<#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>
```

此輸出包括有關包含不安全功能的模組、父命令或配置（如果這是巢狀配置）、已標籤的特定CLI命令、標籤為不安全的原因以及更正該命令所必需的補救操作的關鍵資訊。

使用者還可以使用show system insecure profile 命令檢視所有不安全的CLI模式的綜合清單。 當show system insecure configuration顯示當前應用的限制階段不安全配置時，show system insecure profile顯示系統要檢測的所有限制階段不安全配置。 隨著安全最佳實踐的不斷發展，配置檔案中的不安全配置清單會隨著時間的推移而更新。

常見不安全配置的補救示例

這些示例演示了使用者如何檢測、識別和補救幾種常見的不安全配置。 無論使用者是利用INSECURE_CONFIG系統日誌消息還是show system insecure configuration輸出，思科都實施了軟體來幫助儘可能輕鬆地識別和緩解。

不安全檔案傳輸方法

以下是在裝置上看到的警告訊息：

```
%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
```

您可以運行show system insecure configuration來檢視有關這些不安全配置的其他資訊：

```
<#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#
```

這些日誌直接對映到以下配置：

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

使用者可以通過以下更改緩解不安全配置：

```
<#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
```

不安全舊版SNMP協定

這是裝置上顯示的警告消息：

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

您可以運行show system insecure configuration來檢視有關不安全配置的其他資訊：

```
<#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#
```

這些日誌直接對映到此配置：

<#root>

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

snmp-server community
```

RO

客戶可以使用具有驗證和加密(authPriv)的SNMPv3進行補救。

常見問題 (FAQ)

Q:思科為什麼進行這些更改？

答：思科正在進行這些更改，通過禁用不安全的傳統功能、引入更強大的保護和監控以及簡化安全操作，來增強其網路基礎設施的安全性和恢復能力。這些努力有助於保護客戶免受不斷演變的網路威脅、減少停機時間，並使網路做好應對未來挑戰（如量子計算）的準備。總體而言，該計畫的目標是為當前和未來技術構建一個現代、安全和可靠的基礎

Q:當具有不安全配置的裝置在限制階段升級至該功能的發行版時，會發生什麼情況？

A:當裝置升級為給定功能的限制（第二階段）發行版時，系統在引導過程中檢測不安全的配置，並自動將裝置轉換到不安全模式。

Q:當具有不安全配置的裝置在刪除階段升級至該功能的發行版時，會發生什麼情況？

A:當裝置升級至給定功能的移除（第三階段）版本時，移除的配置不再可用。使用者必須遵守標準遷移過程來管理過時的命令。

Q:在同一版本中是否刪除了所有不安全的功能？

答：同一版本中並未刪除所有不安全的功能。思科堅持分階段的方法，在以下三個階段淘汰不安全功能：首先在配置或檢測到不安全功能時發出警告，然後通過預設禁用這些功能或要求顯式管理員操作（通過引入不安全模式）來限制其使用，最後在未來的版本中完全刪除這些功能。某些功能可以跳過「限制」階段，直接從「警告」移至「刪除」。刪除的時間因功能和平台而異，警告、限制和刪除的版本號因作業系統而異，如Cisco IOS XE、Cisco IOS XR、Cisco NXOS、Cisco ISE和Cisco ASA/FTD。此分步流程可確保將中斷降至最低，並使客戶有時間過渡到安全的替代方案。

Q:我的不安全功能何時進入限制或刪除階段？

答：不安全功能進入「限制」或「刪除」階段的時間因功能和作業系統而異。有關詳細資訊，請參閱功能棄用和刪除詳細資訊文檔。

Q:我的特定不安全功能存在哪些替代方案？

A:客戶可以參閱功能刪除和建議替代方案文檔，確定各種不安全功能和協定的建議替代方案。

Q:如何檢視我目前應用了哪些不安全配置？

答：若要檢視您目前應用的限制階段不安全配置，您可以在Cisco IOS XE 26.1.1及更高版本上使用命令show system insecure configuration。此命令提供裝置上配置的限制階段不安全功能的綜合清單。此外，在Cisco SD-WAN Manager中，您可以導航到Monitor > Advisories，然後選擇Insecure Configurations頁籤，以跨裝置、配置組和模板檢視不安全的配置，並連結至補救步驟。此檢視大約每30分鐘刷新一次，以確保獲得最新資訊。

Q:如何檢視給定軟體版本上所有可能的不安全配置的清單？

A:您可以使用命令show system insecure profile檢視系統要檢測的所有限制階段不安全CLI模式的完整清單。與show system insecure configuration（僅顯示當前應用的不安全配置）不同，配置檔案輸出包括限制階段中所有已知的不安全配置，並會隨著安全最佳實踐的發展而更新。

Q:我更正了一個不安全的配置。 為什麼它仍然顯示在show system insecure configuration輸出中？

答：在不安全的模式下，對不安全配置的掃描僅定期運行。這意味著在糾正不安全的配置後，系統無法立即反映更改，直到進行下一次計畫掃描（30分鐘間隔內進行）。此計畫可確保定期更新和顯示最新的不安全配置詳細資訊，同時最大限度地減少執行掃描所需的開銷。 您可以使用test system secure all命令強制立即重新掃描，這樣您就不必等待掃描計時器過期。

Q:如何主動檢查升級前應用了哪些不安全配置？

答：要主動檢查您在升級之前應用了哪些不安全配置，在Cisco IOS XE 17.18.2之前，客戶可以使用Cisco Resilient Infrastructure頁面上提供的Cisco AI Assistant for Support bot，該頁面允許上傳配置以識別不安全功能。類似工具，Cisco Config Resilient Infrastructure Tester是客戶的另一個選項。 從Cisco IOS XE 17.18.2及更高版本開始，客戶仍可以使用這些工具，但您也可以在您的裝置上直接運行show system insecure configuration命令，以檢視當前應用的不安全配置。但是，使用AI Assistant for Support bot和Resilient Infrastructure Tester提供除直接CLI命令之外的額外的AI驅動增強功能。

其他資源

我們鼓勵客戶閱讀此文檔，以補充對其最佳安全實踐和替代現有不安全配置的理解。

思科彈性基礎架構 — 提供跨思科裝置向增強的安全狀態過渡的基本背景，使用者可利用此頁右下角的Cisco AI Assistant for Support Bot逐步執行指導式工作流程，從各種輸出中識別不安全配置

Cisco Config Resilient Infrastructure Tester — 可用於根據提供的運行配置檢查不安全配置的工具

Cisco IOS XE軟體加固指南 — 詳細介紹強化Cisco IOS XE裝置並提高網路整體安全性的最佳實踐

功能刪除和建議備選方案 — 記錄計畫最終刪除的不安全功能和協定以及建議替代方案的清單

功能棄用和移除詳細資訊 — 當特定不安全功能和通訊協定進入基於Cisco IOS XE軟體版本的警告和/或限制階段時的檔案

SD-WAN監控和維護指南 — Insecure Configuration Management章節 — 介紹對Cisco Catalyst SD-WAN中的不安全功能配置的集中可視性和可操作的補救，幫助管理員識別和修復漏洞，以增強網路安全和維護合規性

可復原的基礎設施：Cisco Catalyst SD-WAN和路由技術參考 — Cisco Catalyst SD-WAN和路由的安全加固和恢復手冊。它提供規範指導，以跨基於CLI和UI的管理模型識別、修復和替換不安全的配置，旨在通過從不安全選項過渡到安全、可復原的替代選項來加強安全性、減少攻擊面，並保護資料，同時確保跨操作模型的一致性

Cisco C9000交換Cisco IOS XE — 彈性基礎設施手冊 — 專注於識別不安全配置，並用安全、彈性的替代方案替代它們，以增強安全狀態、減少攻擊面和保護資料。該攻略旨在確保CLI和UI操作模型的一致性，同時增強Catalyst 9000系列的網路恢復能力和操作簡便性

思科9800無線彈性基礎設施 — 概述思科分階段採取的策略，以淘汰不安全的功能和協定，提供全面的遷移路徑以確保替代方案，防止軟體升級期間服務中斷。它包括跨行傳輸、檔案傳輸和管理協定受影響配置的詳細參考表，以及關於未能遷移的潛在操作影響的指導

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。