IOS XEデバイスの復元力のあるインフラストラクチャについて

内容

はじめに

このドキュメントでは、Secure-by-defaultとSecure-by-designに基づく復元力のあるインフラストラクチャに対するシスコのアプローチについて説明します。

前提条件

要件

このドキュメントに固有の要件はありませんが、Cisco IOS ® XEソフトウェアの基本的な知識は非常に役立ちます。

使用するコンポーネント

このドキュメントの情報は、Cisco IOS XE 17.18.2以降のソフトウェアを実行できるすべてのデバイスに適用されます。これには、Cisco IOS XEルータ、スイッチ、およびWLCが含まれます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

目標

シスコの目標は、シスコのネットワーキング製品に対する攻撃を受ける危険性を大幅に減らし、安全なデフォルト設定、安全でないレガシーテクノロジーと機能の削除、および製品セキュリティの強化によって、セキュリティの脆弱性を最小限に抑えることです。

ネットワークセキュリティポスチャを改善するためのシスコのプッシュに関する詳細については、『Resilient Infrastructure』ドキュメントと『Cisco IOS XE Software Hardening Guide』を参照してください。 ただし、このドキュメントでは、これらの重要なセキュリティ変更を段階的に実装した結果として生じる技術的な側面と考慮事項に主に焦点を当てています。

段階的アプローチ

攻撃を受ける可能性を減らし、重要なセキュリティベストプラクティスを採用すると同時に、お客様の混乱と作業を最小限に抑えるため、シスコは段階的なアプローチを採用して、安全でない機能とプロトコルを削除しています。 安全でない設定のフェーズは、機能またはプロトコルに固有であることに注意してください。 ある機能は警告フェーズに残り、別の機能は制限フェーズに入ります。

フェーズ1：警告

安全でない主要機能を設定すると、ユーザはCLIで警告を受け取ります。 シスコの目標は、お客様がより安全なオプションへの移行を計画できるように、こうした安全でない設定に対する認識を高めることです。 シスコでは、安全でない警告メッセージにはただちに対処することを強く推奨します。 警告フェーズで安全でない設定がトリガーされることはなく、安全でないモードが必要になることもありません。

Cisco IOS XEバージョン17.18.2は、安全でない機能に対して警告フェーズを導入した最初のソフトウェアリリースです。

フェーズ2：制限事項

安全でない主要な機能はデフォルトで無効になっており、有効にするには明示的なユーザアクションが必要です（安全でないモードの導入により）。 既存の展開は引き続き機能しますが、新規インストールでは、これらの安全でない設定を意図的に有効にする必要があります。 Cisco IOS XEプラットフォームの一部の機能には、制限フェーズを設定できないことに注意してください。 制限フェーズでは、

その後の削除の前に、いくつかのリリースに関する警告を表示するだけです。

Cisco IOS XEバージョン26.1.1は、安全でない機能に制限フェーズを導入した最初のソフトウェアリリースです。

フェーズ3：削除

古い安全でない機能は完全に削除されます。 機能を削除するタイミングは、ユーザへの影響と導入によって異なります。 たとえば、SNMPv2などの広く採用されている機能は、あまり一般的に使用されていない機能よりも段階的に廃止されます。

Cisco IOS XEバージョン26.2.1は、安全でない機能の削除フェーズを導入した最初のソフトウェアリリースです。

主なコマンド

これらのコマンドは、復元力の高いインフラストラクチャを実装しているお客様に非常に便利で

す。 これらのコマンドは、このドキュメント全体を通じて参照されています。

- show system insecure configuration（隠しコマンド）
  - このコマンドは、現在適用されている、制限フェーズにある安全でない設定を表示するために使用されます。 警告フェーズや削除フェーズにある安全でない設定は表示されません。 このコマンドでは、次回の安全でない設定スキャンの残り時間も表示されます（「タイマーと安全でない設定スキャン」セクションで詳しく説明）。
- show system securityモード
  - このコマンドは、デバイスがセキュアモードか非セキュアモードかを示す簡単な出力を提供します。
- show running-config all | include system mode insecure（システムモードが安全でない場合）
  - このコマンドは、システムモードの非セキュアキーワードでフィルタリングされた実行コンフィギュレーション（デフォルト設定を含む）を表示します。 詳細については、「セキュリティモードの変更」セクションを参照してください。
- システムのセキュリティをすべてテスト
  - このコマンドは、非セキュアな設定スキャンをただちに実行し、show system insecure configurationの出力を表示します。 これは、スキャンタイマーの期限切れを待たずに、変更の後に安全でないフラグの付いた設定を更新するのに役立ちます。
- show system insecure profile（隠しファイル）
  - このコマンドは、そのバージョンのソフトウェアで検出するようにシステムが設計されている、制限フェーズの安全でない設定を表示します。 プロファイル内の安全でない設定のリストは、セキュリティのベストプラクティスが進化し続けるにつれて更新されます。 これは、デバイスで現在設定されている安全でない機能を反映するものではありません。 これは、システムが検出したすべての制限フェーズの安全でない設定の単なるリストです。 すべてのベストプラクティスについては、「その他のリソース」セクションの「強化ガイド」を参照してください。

注意事項と考慮事項

タイマーと安全でない設定スキャン

このドキュメントで詳述されている安全でない設定チェックと警告メッセージは、タイマーの実行頻度を制限するタイマーに基づいてスケジュールされます。 安全でない設定が修正されても、show system insecure configurationの出力からすぐには消えません。 設定スキャナは30分サイクルで動作するため、最大30分の遅延があります。 同様に、安全でない設定を適用してから、対応する%SYS-4-INSECURE_CONFIG syslogを適用するまでに、最大2分の遅延が発生する可能性があります。

ユーザは、show system insecure configurationコマンドを使用して、次のスキャンが実行されるまでの残り時間を表示できます。 タイマーは、出力の最初のセクションに表示されます。 この最初の例は、設定変更が行われ、安全でない設定に対する次のスキャンが8分後に行われることを

示しています。

```
<#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>
```

次の例は、前回のスキャン以降は設定変更が検出されていないため、安全でない設定を追加でチェックする必要がないことを示しています。

```
<#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>
```

test system secure allコマンドを使用すると、即時に再スキャンを強制できます。 このコマンドでは、即時の再スキャンを促すだけでなく、show system insecure configurationの出力も表示さ

れます。 これは、スキャンタイマーの期限切れを待たずに、変更の後に安全でないフラグの付いた設定を更新するのに役立ちます。

安全でない設定の警告

17.18.2以降では警告フェーズが導入されており、ユーザは次のsyslog構文を確認できます。

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

次のようなメッセージが表示されます。

- モジュール：ログメッセージを生成したコンポーネント（LOGGING、HTTP、LINEなど）
- コマンド：警告メッセージをトリガーした特定の設定
- Reason：この設定が非セキュアとしてフラグが付けられている理由。
- 修復：より安全な方法に移行するために必要な措置

これらの警告メッセージは、デバイスのサービスや機能に影響を与えません。 この目的は、このような安全でない設定に注意を向け、ユーザが予防的に設定を緩和できるようにすることです。

注：Cisco IOS XEバージョン26.1.1以降では、INSECURE_DYNAMIC_WARNINGメッセージは警告フェーズの安全でない設定を示し、INSECURE_CONFIGメッセージは制限フェーズの安全でない設定を示します。 show system insecure configurationの出力には、制限フェーズの設定だけが表示されます。

これらのログは、ブート時、または安全でない設定を適用した後に表示されることに注意してください。 また、定期的にデバイスに表示することもできます。 これらのメッセージとその構文の詳細については、『耐障害性インフラストラクチャCisco IOS XEセキュリティ警告リファレンス』を参照してください。

設定直後のSyslogの例

これらは、非セキュアな設定を適用した直後に表示されるsyslogメッセージの例です。 「タイマーと安全でない設定スキャン」セクションで説明したように、安全でない設定を適用した後、これらのメッセージが表示されるまでに最大2分かかることがあります。

```
! 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
```

ブートアップ時のsyslogの例

ブートアップ時に表示されるメッセージ例を次に示します。 システムが検出した安全でない設定ごとに、次のメッセージが表示されます。

```
! 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
```

非セキュアモード

非セキュアモードは、Cisco IOS XEバージョン26.1.1以降で導入されました。非セキュアモードは、既存の安全でない導入と将来の強化されたネットワークとの間のギャップを埋めるために存在します。非セキュアモード設定を追加すると、お客様は既存の非セキュアな機能を引き続き使用しながら、セキュリティリスクを引き起こして軽減する必要のある設定をフラグ付けできます。また、工場出荷時のデフォルトのデバイスに適用する前に、安全でない機能の確認応答としても機能します。 安全でないモードでは、フェーズ3より前に廃止された機能を完全に削除するサポート終了計画も可能です。セキュアでないモードの目標は、機能の中断を最小限に抑えながら、お客様をセキュアな設計に基づくネットワークに移行することです。

工場出荷時のデフォルトである新規の導入と新規インストールでは、デフォルトでセキュアモードが設定されています(非セキュアシステムモードなし)。つまり、デバイスで制限フェーズの非セキュアな設定をユーザが適用できなくなります。ユーザは、制限フェーズで安全でない機能とプロトコルを適用するために、system mode insecureグローバルコンフィギュレーションで安全でないモードを明示的に有効にする必要があります。 警告フェーズで安全でない機能とプロトコルは、セキュアモードでも適用できますが、警告メッセージが生成されます。

現在のセキュリティモードの確認

ユーザはshow system security modeコマンドを使用して、デバイスがセキュアモードか非セキュアモードかを確認できます。show running-config all | include system modeコマンドは、デバイスがセキュアモードか非セキュアモードかについても反映します。 allキーワードは、デフォルト設定を出力に含めるようにデバイスに指示します。これは、新規導入ではセキュアモードがデフォ

ルト設定であるためです。

次の出力には、セキュアモードのデバイスが反映されています。

```
<#root>
Device#

show system security mode


System Security Mode :

Secure



Device#

show running-config all | include system mode



no system mode insecure
```

デバイスが非セキュアモードになっているかどうかを確認するには、同じコマンドを使用できます。

```
<#root>
Device#

show system security mode


System Security Mode :

Insecure



Device#

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

```
system mode insecure
```

セキュリティモードの変更

非セキュアモードの有効化

ユーザは、system mode insecureグローバルコンフィギュレーションで、非セキュアモードをイネーブルにできます。

<#root>

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

system mode insecure
```

セキュアモードの有効化

ユーザは、no system mode insecureグローバルコンフィギュレーションでセキュアモードをイネーブルにできます。

<#root>

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

no system mode insecure
```

セキュアモードを有効にするための要件

セキュアモードに移行するには、次の手順を実行します。

- 安全でない設定のスキャンを完了する必要があります。
- すべての安全でない設定をデバイスから削除する必要があります

セキュリティで保護されていない設定のスキャンが完了しない場合、スキャンタイマーの期限が切れた後に再試行するよう求めるメッセージが表示されます。

<#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.

test system secure allコマンドを使用すると、即時に再スキャンを強制できます。

タイマーが切れて設定スキャンが完了した後も、システムが安全でない設定を検出すると、システムはセキュアモードに移行しません。 システムがセキュアモードに入る前に、これらの安全でない設定を削除する必要があります。

<#root>

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

insecure cli(s) are present in system.

これらの要件が両方とも満たされると、ユーザはセキュアモードを有効にすることができます。

<#root>

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

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

安全でない設定の適用

セキュアモードでは、ユーザが制限フェーズの安全でない設定を適用しようとすると、エラーメッセージが表示され、設定は適用されません。 例：

<#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
```

設定試行の直後に表示されるメッセージには、デバイスがセキュアモードであることが示されます。したがって、提供されている安全でない設定は適用できません。 安全でない設定が適用されなかったことを確認できます。

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

制限フェーズの安全でない設定を適用するには、ユーザは最初に、システムモードの安全でないグローバルコンフィギュレーションで、安全でないモードを明示的に有効にする必要があります。

<#root>

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

system mode insecure


Device(config)# end

Device#show running-config all | include system mode

system mode insecure
```

デバイスが非セキュアモードになると、制限フェーズの非セキュア設定を適用できます。 同様のセキュリティ警告メッセージが設定時に表示されますが、安全でない設定が適用されます。

<#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#
```

ユーザには、安全でない設定に注意を促す警告メッセージも表示されます。 これらのメッセージをレート制限するためにキューに入れるタイマーのため、このsyslogが設定されてから表示されるまでに最大2分かかることがあります。

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

制限フェーズの機能とプロトコルのみが、非セキュアモードを要求またはトリガーすることに注意してください。 警告フェーズにある機能とプロトコルは、引き続きセキュアモードで適用できます

非セキュアモードへの自動移行

Cisco IOS XEデバイスを26.1.1以降にアップグレードすると、システムはブートプロセス中に制限フェーズの安全でない設定を検出し、デバイスを安全でないモードに自動的に移行します。ユーザがsystem mode insecureグローバル設定を自分で手動で追加する手間は不要で、制限フェーズに移行する際に安全でない機能への影響はありません。

この例では、17.18.2（非セキュアモードコンテキストがない）から26.1.1（明示的な非セキュアモードコンテキストがある）へのアップグレード中の非セキュアモードへの自動移行について説明します。 デバイスは、非セキュアなip ftp source-interface GigabitEthernet0/0/0設定が適用された状態で起動します。

最初は、このデバイスはCisco IOS XEバージョン17.18.2で起動します。

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

安全でない設定が1つ検出されました。

<#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>
```

また、このバージョンにはセキュアモードと非セキュアモードの概念はありません。

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

その後、デバイスを26.1.1にアップグレードすると、セキュアモードと非セキュアモードが導入されます。

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

同じ安全でない設定が適用されます。

<#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>
```

この（または任意の）制限フェーズの安全でない設定が存在するため、システムは安全でないモードを検出し、自動的に移行します。

<#root>

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

Insecure
```

system mode insecure設定が自動的に適用されます。

<#root>

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

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


system mode warning periodicity 24
Device#
```

注意：警告フェーズの安全でない設定が存在しても、安全でないモードに移行することはありません。 制限フェーズの安全でない設定が存在する場合にのみ、自動移行がトリガーされます。

デバイスの強化

削除フェーズ（フェーズ3）に入る前に、安全でない機能やプロトコルから、より安全な方法に移行するよう、あらゆる努力を払うことを強く推奨します。 シスコは、安全でない設定を特定し、簡単に修正できるようにするため、いくつかのサービサビリティ拡張機能を統合しました。

適用する安全でない設定の特定

ユーザは、show system insecure configuration EXECコマンドを使用して、現在適用されている制限フェーズの安全でない設定を表示できます。 このコマンドは、バージョン26.1.1以降ではshow tech-supportの出力に自動的に含まれます。 次に、3つの制限フェーズの安全でない設定が適用されたデバイスからの出力例を示します。

<#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>
```

この出力には、非セキュアな機能を含むモジュールに関する重要な情報、ネストされた設定の場合の親コマンドまたは設定、フラグが付けられた特定のCLIコマンド、非セキュアとマークされた理由、および修正するために必要な修復操作が含まれます。

また、ユーザはshow system insecure profileコマンドを使用して、すべての非セキュアCLIパターンの包括的なリストを表示することもできます。 show system insecure configurationは、現在適用されている制限フェーズの安全でない設定を示しますが、show system insecure profileは、システムが検出するように設計されているすべての制限フェーズの安全でない設定を表示します。プロファイル内の安全でない設定のリストは、セキュリティのベストプラクティスが進化し続けるにつれて更新されます。

一般的な安全でない設定の修復例

次の例は、一般的に発生する安全でない設定を検出、特定、および修復する方法を示しています。 シスコでは、ユーザがINSECURE_CONFIG syslogメッセージやshow system insecure configurationの出力を利用しているかどうかにかかわらず、識別と緩和を可能な限り簡単に行えるようにソフトウェアを実装しています。

安全でないファイル転送方法

デバイスに表示される警告メッセージは次のとおりです。

```
%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
```

show system insecure configurationを実行すると、これらの非セキュアな設定に関する追加情報を表示できます。

<#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#
```

これらの口グは、次の設定に直接マッピングされます。

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

ユーザは、次の変更によって安全でない設定を緩和できます。

<#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
```

安全でないレガシーSNMPプロトコル

デバイスに次の警告メッセージが表示されます。

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

show system insecure configurationを実行して、非セキュアな設定に関する追加情報を確認できます。

```
<#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#
```

次の口グは、この設定に直接マッピングされます。

<#root>

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

snmp-server community
```

RO

この問題は、SNMPv3 with authentication and encryption(authPriv)を使用して修正できます。

よく寄せられる質問（FAQ）

Q：シスコはなぜ今回の変更を行うのですか。

A：シスコは、ネットワークインフラストラクチャのセキュリティと復元力を強化するためにこれらの変更を行っています。具体的には、安全性の低いレガシー機能を無効にし、強力な保護とモニタリングを導入し、安全な運用を簡素化します。これらの取り組みは、進化するサイバー脅威からお客様を保護し、ダウンタイムを短縮し、量子コンピューティングのような将来の課題にネットワークを準備するのに役立ちます。全体として、このイニシアチブは現在および将来のテクノロジーのための現代的で安全かつ信頼性の高い基盤の構築を目指しています

Q：安全でない設定のデバイスが、その機能の制限フェーズでリリースにアップグレードされるとどうなりますか。

A：デバイスが特定の機能の制限（フェーズ2）リリースにアップグレードされると、システムは

ブートプロセス中に安全でない設定を検出し、自動的にデバイスを安全でないモードに移行します。

Q：安全でない設定のデバイスが、その機能の削除フェーズでリリースにアップグレードされるとどうなりますか。

A：特定の機能に関して、デバイスを削除（フェーズ3）リリースにアップグレードすると、削除された設定は使用できなくなります。古いコマンドを管理するには、標準の移行手順に従う必要があります。

Q：同じリリースで、セキュリティで保護されていないすべての機能が削除されるのですか。

A：同じリリースでは、セキュリティで保護されていない機能がすべて削除されるわけではありません。シスコでは、セキュリティで保護されていない機能を3段階で廃止する段階的アプローチを採用しています。まず、セキュリティで保護されていない機能が設定または検出されたときに警告を発行し、次にデフォルトで無効にするか明示的な管理者アクションを要求して使用を制限し（セキュリティで保護されていないモードの導入により）、最後に将来のリリースで完全に機能を削除します。一部の機能では、制限フェーズをスキップして、警告から削除に直接移行できます。削除のタイミングは機能とプラットフォームによって異なり、警告、制限、および削除のリリース番号はCisco IOS XE、Cisco IOS XR、Cisco NXOS、Cisco ISE、およびCisco ASA/FTDなどのオペレーティングシステムによって異なります。この段階的なプロセスにより、中断が最小限に抑えられ、お客様は安全な代替案に移行する時間を確保できます。

Q：セキュリティで保護されていない機能が制限または削除フェーズに移行するのはいつですか。

A：保護されていない機能が制限または削除フェーズに移行するタイミングは、機能やオペレーティングシステムによって異なります。詳細については、『機能の廃止と削除の詳細』を参照してください。

Q：安全でない特定の機能に対して、どのような代替手段がありますか。

A：お客様は『機能の削除と代替案』のドキュメントを参照して、さまざまな安全でない機能とプロトコルに対する推奨案を確認できます。

Q：現在適用されている安全でない設定を確認するには、どうすればよいのですか。

A：現在適用されている制限フェーズの安全でない設定を確認するには、Cisco IOS XE 26.1.1以降のリリースでコマンドshow system insecure configurationを使用します。このコマンドは、デバイスで設定されている制限フェーズの安全でない機能の包括的なリストを提供します。また、Cisco SD-WAN Managerでは、Monitor > Advisoriesに移動し、Insecure Configurationsタブを選

択して、デバイス、設定グループ、およびテンプレートにわたる安全でない設定を表示できます。また、修復手順へのリンクも表示されます。このビューは約30分ごとに更新され、最新情報が確認されます。

Q：特定のソフトウェアバージョンで発生する可能性があるすべての安全でない設定のリストを表示するには、どうすればよいのですか。

A：コマンドshow system insecure profileを使用すると、システムが検出するように設計されているすべての制限フェーズの安全でないCLIパターンの完全なリストを表示できます。現在適用されている安全でない設定のみを表示するshow system insecure configurationとは異なり、プロファイル出力には制限フェーズでの安全でない既知の設定がすべて含まれ、セキュリティのベストプラクティスが発展するのに合わせて更新されます。

Q：安全でない設定を修正しました。 なぜ、show system insecure configurationの出力に、このコマンドが引き続き表示されるのですか。

A：安全でない設定のスキャンは、安全でないモードの間だけ定期的に実行されます。つまり、安全でない設定を修正した後、30分の間隔で次のスケジュールされたスキャンが実行されるまで、システムは変更を即座に反映できません。このスケジューリングにより、スキャンの実行に必要なオーバーヘッドを最小限に抑えながら、最新の安全でない設定の詳細が定期的に更新および表示されるようになります。 test system secure allコマンドを使用すると、即時に再スキャンを強制できるため、スキャンタイマーが切れるまで待つ必要がありません。

Q：アップグレードの前に、適用した安全でない設定を予防的に確認するにはどうすればよいのですか。

A:Cisco IOS XE 17.18.2より前のバージョンでは、アップグレード前に適用した安全でない設定を予防的にチェックするために、Cisco Resilient Infrastructureページで利用可能なCisco AI Assistant for Supportボットを使用できます。このボットを使用すると、設定をアップロードして安全でない機能を特定できます。同様のツールであるCisco Config Resilient Infrastructure Testerも、お客様にとってのもう1つのオプションです。 Cisco IOS XE 17.18.2以降からは、これらのツールを使用できますが、デバイスでshow system insecure configurationコマンドを直接実行して、現在適用されている安全でない設定を表示することもできます。ただし、AI Assistant for SupportボットとResilient Infrastructure Testerを使用すると、直接CLIコマンドを使用する以外にも、AIを活用した強化機能が追加されます。

関連情報

セキュリティのベストプラクティスや、セキュリティで保護されていない既存の設定に対する代替策についての理解を深めるには、このドキュメントをお読みになることをお勧めします。

Cisco Resilient Infrastructure：シスコデバイス間で強化されたセキュリティポスチャへの移行に関する重要な背景情報を提供します。ユーザはこのページの右下隅にあるCisco AI Assistant for Supportボットを利用してガイド付きワークフローを実行し、さまざまな出力から安全でない設定を特定できます

Cisco Config Resilient Infrastructure Tester：提供されたrunning-config

Cisco IOS XEソフトウェア強化ガイド:Cisco IOS XEデバイスを強化し、ネットワーク全体のセキュリティを強化するためのベストプラクティスの詳細を示します

Feature Removal and Suggested Alternative：最終的な削除が計画されている、安全でない機能とプロトコルのリスト、および推奨される選択肢を文書化します

機能の廃止と削除の詳細:Cisco IOS XEソフトウェアバージョンに基づき、特定の安全でない機能およびプロトコルが警告または制限フェーズに入ったときのドキュメント

SD-WAN Monitor and Maintain Guide - Insecure Configuration Management Chapter：管理者がネットワークセキュリティを強化し、コンプライアンスを維持するために脆弱性を特定して修正できるようにする、Cisco Catalyst SD-WANの安全でない機能設定に対する中央集中型の可視性と実用的な修復方法について説明します

復元力のあるインフラストラクチャ：Cisco Catalyst SD-WANおよびルーティングテクニカルリファレンス – Cisco Catalyst SD-WANおよびルーティングのセキュリティ強化および復元力プレイブック。CLIおよびUIベースの管理モデル間で安全でない構成を特定、修正、および置き換えるための規範的ガイダンスを提供し、運用モデル間の一貫性を確保しながら、安全でない構成から安全で復元力のある構成に移行することで、セキュリティを強化し、攻撃対象領域を縮小し、データを保護することを目的としています

Cisco C9000スイッチングCisco IOS XE：復元力のあるインフラストラクチャプレイブック：安全でない設定を特定し、その設定を安全で復元力のある代替ソリューションに置き換えることで、セキュリティポスチャを強化し、攻撃対象領域を縮小し、データを保護することに重点を置いています。このプレイブックの目的は、Catalyst 9000ファミリのネットワークの復元力と運用の簡素化を強化しながら、CLIおよびUI運用モデル全体で一貫性を確保することです

Cisco 9800 Wireless Resilient Infrastructure：安全でない機能とプロトコルを廃止するためのシスコの段階的な戦略の概要を示し、ソフトウェアのアップグレード中のサービス中断を防ぐために安全な代替手段への包括的な移行パスを提供します。これには、ライントランスポート、ファイル転送、および管理プロトコルにわたる影響を受ける構成の詳細な参照テーブルと、移行に失敗した場合の潜在的な運用上の影響に関するガイダンスが含まれます

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。