了解IOS XE设备上的弹性基础设施

目录

简介

本文档介绍思科的弹性基础设施方法，该方法植根于默认安全方法和设计安全方法。

先决条件

要求

虽然本文档没有具体要求，但对Cisco IOS ® XE软件的基本了解非常有帮助。

使用的组件

本文档中的信息适用于可以运行Cisco IOS XE 17.18.2及更高版本软件的所有设备。其中包括Cisco IOS XE路由器、交换机和WLC。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

目标

我们的目标是通过安全的默认设置、删除不安全的传统技术和功能，以及增强产品安全性，有效减少思科网络产品的攻击面，并最大限度地减少安全漏洞。

在弹性基础设施文档以及Cisco IOS XE软件加固指南中，您可以找到有关思科为改善网络安全状态而推出的更多详细信息。但是，本文档主要侧重于这些重要安全更改分阶段实施所带来的技术方面和注意事项。

分阶段方法

为了确保减少攻击面，采用关键的安全最佳实践，同时最大限度地减少客户的中断和工作量，思科采用分阶段的方法来消除不安全的功能和协议。 请注意，非安全配置的阶段划分是特定于功能或协议的。 一个功能可以保留在“警告”阶段，而另一个功能进入“限制”阶段。

第一阶段：警告

配置主要不安全功能时，用户会在CLI上收到警告。 我们的目标是提高对不安全配置的认识，以便客户可以开始计划迁移到更安全的选项。 思科强烈建议立即处理所有不安全的警告消息。 处于警告阶段的不安全配置不会触发或需要不安全模式。

Cisco IOS XE版本17.18.2是第一个对不安全功能引入警告阶段的软件版本。

第二阶段：限制

默认情况下会禁用主要不安全功能，并需要明确的用户操作才能启用（通过引入不安全模式）。 现有部署将继续运行，但新安装需要特意启用这些不安全的配置。 请注意，Cisco IOS XE平台上的某些功能不能处于限制阶段：他们可以

在后续移除之前只显示几个版本的警告。

Cisco IOS XE版本26.1.1是第一个针对不安全功能引入限制阶段的软件版本。

第三阶段：删除

完全删除过时的不安全功能。 功能删除的时间因用户影响及采用情况而异。 例如，广泛采用的功能（如SNMPv2）的淘汰速度比不常用的功能慢。

Cisco IOS XE版本26.2.1是第一个针对不安全功能引入删除阶段的软件版本。

关键命令

当客户实施恢复能力更强的基础设施时，这些命令非常有用。 本文档中会引用这些命令。

- show system insecure configuration
  - 此命令用于显示处于限制阶段的当前应用的不安全配置。 它不会显示处于警告阶段或移除阶段的不安全配置。 此命令还显示下一次不安全的配置扫描的剩余时间（在“计时器和不安全的配置扫描”部分中详细介绍）。
- show system security mode
  - 此命令提供显示设备处于安全模式或不安全模式的简短输出。
- show running-config all | include system mode insecure
  - 此命令显示按系统模式不安全关键字过滤的运行配置（包括默认配置）。 请参阅“更改安全模式”部分或其他详细信息。
- test system secure all
  - 此命令立即运行不安全的配置扫描并显示show system insecure configuration输出。 这有助于在更改后刷新不安全标记的配置，而无需等待扫描计时器过期。
- show system insecure profile
  - 此命令显示系统在该软件版本上用于检测的Restriction-phase insecure配置。 随着安全最佳实践的持续发展，配置文件中的不安全配置列表会不断更新。 这并不能反映设备上当前配置的不安全功能。 它只是系统检测到的所有限制阶段不安全配置的列表。 有关所有最佳安全实践，请参阅“其他资源”部分中的“强化指南”。

注意事项和注意事项

计时器和不安全的配置扫描

本文档中详细介绍的不安全配置检查和警告消息都安排在计时器上，以限制其运行频率。 更正不安全的配置后，它不会立即从show system insecure configuration输出中消失。 配置扫描仪以30分钟的周期运行，因此存在长达30分钟的延迟。 同样，在应用不安全的配置与其对应的%SYS-4-INSECURE_CONFIG系统日志之间最多可能会存在两分钟的延迟。

用户可以使用show system insecure configuration命令查看下一次扫描运行前的剩余时间。 计时器显示在输出的第一部分中。 第一个示例显示已进行配置更改，并且在8分钟内对不安全的配置进行下一次扫描：

```
<#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>
```

下一个示例显示自上次扫描以来未检测到任何配置更改，因此无需对不安全的配置进行其他检查：

```
<#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>
```

用户可以使用test system secure all命令强制立即重新扫描。 除了提示立即重新扫描之外，此命令还显示show system insecure configuration输出。这有助于在更改后刷新不安全标记的配置，而无需等待扫描计时器过期。

不安全的配置警告

从17.18.2开始引入警告阶段，用户可以看到以下系统日志语法：

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

这些消息包括：

- 模块:生成日志消息的组件（例如LOGGING、HTTP或LINE）
- 命令:触发警告消息的特定配置
- 理由：此配置标记为不安全的原因
- 补救:迁移至更安全的替代方案所需的操作

这些警告消息不会影响设备上的服务或功能。 目的是提醒用户注意这些不安全的配置，以便用户主动缓解这些配置。

注意：从Cisco IOS XE版本26.1.1开始，INSECURE_DYNAMIC_WARNING消息在警告阶段指示不安全的配置，而INSECURE_CONFIG消息在限制阶段指示不安全的配置。 show system insecure configuration输出中仅显示Restriction-phase配置。

请注意，这些日志在启动时或在应用不安全的配置后可见。 此外，它们可以定期重新出现在设备上。 有关这些消息及其语法的更多详细信息，请参阅弹性基础设施Cisco IOS XE安全警告参考。

配置后不久出现的系统日志示例

以下是应用不安全的配置后不久出现的系统日志消息示例。 如“计时器和不安全配置扫描”部分中所述，应用不安全配置后，可能需要最多两分钟才会显示以下消息：

```
! 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
```

启动时看到的系统日志示例

这些是启动时显示的示例消息。 对于系统检测到的每个不安全配置，系统都会显示一条消息：

```
! 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

从Cisco IOS XE版本26.1.1开始引入不安全模式。 不安全模式有助于弥合现有不安全部署与未来强化网络之间的差距。添加不安全模式配置后，客户可以继续使用现有的不安全功能进行操作，同时标记哪些配置会带来安全风险并需要加以缓解。在尝试将不安全功能应用到出厂默认设备之前，它还可以充当不安全功能的确认。 不安全模式还允许在第3阶段之前对已弃用的功能进行寿命终止规划，这些功能将在其中完全删除。不安全模式的目的是将客户迁移到按设计提供保护的网络，同时最大限度地减少可能出现的功能中断。

对于出厂默认的全新部署和全新安装，默认情况下会设置安全模式(无系统模式不安全)，这意味着设备不允许用户应用限制阶段不安全的配置。用户需要使用system mode insecure全局配置显式启用不安全模式，以便应用限制阶段不安全的功能和协议。 处于警告阶段的不安全功能和协议仍可在安全模式下应用，但它们确实会生成警告消息。

检查当前安全模式

用户可以使用show system security mode命令检查设备是否处于安全模式或不安全模式。show

running-config all | include system mode命令还反映设备处于安全模式或不安全模式。all关键字告诉设备在输出中包括默认配置，因为安全模式是新部署的默认设置。

以下输出反映了处于安全模式的设备：

```
<#root>
Device#

show system security mode


System Security Mode :

Secure



Device#

show running-config all | include system mode



no system mode insecure
```

相同的命令可用于检查设备是否处于不安全模式：

```
<#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

启用不安全模式

用户可以使用系统模式不安全的全局配置启用不安全模式：

<#root>

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

system mode insecure
```

启用安全模式

用户可以使用no system mode insecure全局配置启用安全模式：

<#root>

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

no system mode insecure
```

启用安全模式的要求

要进入安全模式，请执行以下操作：

- 任何不安全的配置扫描都必须完成，并且
- 必须从设备中删除所有不安全的配置

如果未完成不安全的配置扫描，系统会在扫描计时器过期后提示用户重试：

<#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.
```

用户可以使用test system secure all命令强制立即重新扫描。

如果计时器到期且配置扫描完成后，系统仍检测到任何不安全的配置，则系统不会进入安全模式。必须删除这些不安全的配置，系统才能进入安全模式：

<#root>

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

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

满足这两个要求后，用户可以启用安全模式：

<#root>

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

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

应用不安全的配置

在安全模式下，如果用户尝试应用受限阶段的不安全配置，则会显示错误消息，且不会应用该配置。 例如：

<#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
```

配置尝试后立即显示的消息表明设备处于安全模式，因此无法应用提供的不安全配置。 您可以确认未应用不安全的配置：

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

要应用限制阶段不安全的配置，用户需要首先使用系统模式不安全的全局配置显式启用不安全模式：

<#root>

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

system mode insecure

Device(config)# end

Device#show running-config all | include system mode

system mode insecure
```

一旦设备处于不安全模式，就可以应用限制阶段的不安全配置。 配置时会显示类似的安全警告消息；但是，应用了不安全的配置：

<#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#
```

用户还会看到警告消息，提醒用户注意不安全的配置。 由于用于对这些消息进行排队以限制其速率的计时器，配置后最多可能需要两分钟才能显示此系统日志：

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

请注意，只有处于限制阶段的功能和协议需要或触发不安全模式。 处于警告阶段的功能和协议仍可在安全模式下应用

自动转换到不安全模式

当Cisco IOS XE设备升级到26.1.1或更高版本时，系统在引导过程中检测到任何限制阶段的不安全配置，并自动将设备转换到不安全模式。用户无需担心自己手动添加system mode insecure全局配置，而且在进入Restriction阶段时不会对不安全功能造成任何影响。

此示例介绍从17.18.2（其中没有不安全模式情景）升级到26.1.1（具有显式不安全模式情景）的过程中自动转换到不安全模式。 设备从应用的不安全ip ftp source-interface GigabitEthernet0/0/0配置开始。

最初，此设备从Cisco IOS XE版本17.18.2开始：

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

检测到一个不安全的配置：

<#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，此版本中没有“安全模式”或“不安全模式”的概念：

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

设备随后升级到26.1.1，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
```

仍然应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>
```

由于存在此（或任何）限制阶段不安全配置，系统检测到并自动转换到不安全模式：

```
<#root>

Device# show system security mode
System Security Mode :

Insecure
```

系统模式不安全配置自动应用：

```
<#root>

Device# show running-config all | include system mode

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


system mode warning periodicity 24
Device#
```

请注意，存在警告阶段的不安全配置不会触发向不安全模式的转换。 只有存在限制阶段的不安全配

置才会触发自动转换。

加固设备

强烈建议您尽力在删除阶段（第三阶段）之前从不安全的功能和协议迁移到更安全的方法。 思科集成了一些可维护性增强功能，使识别不安全的配置并纠正它们变得更加容易。

确定应用的不安全配置

用户可以查看当前使用show system insecure configuration EXEC命令应用的限制阶段不安全配置。 此命令自动包含在26.1及更高版本中的show tech-support输出中。 以下是应用了三个限制阶段不安全配置的设备的示例输出：

```
<#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>
```

此输出包括有关包含不安全功能的模块的关键信息、父命令或配置（如果这是嵌套配置）、标记的特定CLI命令、标记为不安全的原因以及更正该命令所需的补救操作。

用户还可以使用show system insecure profile命令查看所有不安全的CLI模式的综合列表。 当show system insecure configuration显示当前应用的限制阶段不安全配置时，show system insecure profile显示系统要检测的所有Restriction-phase insecure配置。 随着安全最佳实践的持续发展，配置文件中的不安全配置列表会不断更新。

常见不安全配置的补救示例

这些示例演示了用户如何检测、识别和补救几种常见的不安全配置。 无论用户是利用INSECURE_CONFIG系统日志消息还是show system insecure configuration输出，思科都实施了软件来帮助尽可能轻松地识别和缓解。

不安全的文件传输方法

以下是在设备上看到的警告消息：

```
%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
```

您可以运行show system insecure configuration来查看有关这些不安全配置的其他信息：

```
<#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#
```

这些日志直接映射到以下配置：

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

用户可以通过以下更改缓解不安全配置：

<#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
```

不安全传统SNMP协议

这是设备上显示的警告消息：

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

您可以运行show system insecure configuration来查看有关不安全配置的其他信息：

<#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#
```

这些日志直接映射到此配置：

<#root>

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

snmp-server community
```

RO

客户可以使用SNMPv3进行身份验证和加密(authPriv)进行补救。

常见问题解答 (FAQ)

问:思科为什么要进行这些更改？

答：思科正在进行这些更改，通过禁用不安全的传统功能、引入更强大的保护和监控，以及简化安全操作，来增强其网络基础设施的安全性和弹性。这些努力有助于保护客户免受不断演变的网络威胁、减少停机时间，并使网络为量子计算等未来挑战做好准备。总体来说，该计划的目的是为当前和未来的技术构建一个现代、安全且可靠的基础

问:当具有不安全配置的设备在限制阶段升级至该功能的版本时，会发生什么情况？

A：当设备升级到给定功能的限制（第二阶段）版本时，系统在引导过程中检测不安全的配置，并自动将设备转换到不安全模式。

问:当具有不安全配置的设备在移除阶段升级至该功能的版本时，会发生什么情况？

A：当设备升级到给定功能的移除（第三阶段）版本时，移除的配置将不再可用。用户必须遵守管理过时命令的标准迁移过程。

问:在同一版本中是否删除了所有不安全的功能？

答：并非所有不安全的功能都会在同一版本中移除。思科坚持采用分阶段方法，在以下三个阶段淘汰不安全功能：首先在配置或检测到不安全功能时发出警告，然后通过默认禁用这些功能或要求管理员采取明确操作（通过引入不安全模式）来限制其使用，最后在未来的版本中完全删除这些功能。某些功能可以跳过“限制”阶段，直接从“警告”移至“删除”。删除时间因功能和平台而异，警告、限制和删除的版本号因操作系统而异，如Cisco IOS XE、Cisco IOS XR、Cisco NXOS、Cisco ISE和Cisco ASA/FTD。此分步流程可确保将中断降至最低，并使客户有时间过渡到安全的替代方案。

问:我的不安全功能何时进入“限制”或“删除”阶段？

答：不安全功能进入限制或移除阶段的时间因功能和操作系统而异。有关详细信息，请参阅功能弃用和删除详细信息文档。

问:我的特定不安全功能存在哪些替代方案？

A：客户可以参阅功能删除和建议替代方案文档，确定各种不安全的功能和协议的建议替代方案。

问:如何查看我当前应用了哪些不安全的配置？

答：若要查看您当前应用了哪些限制阶段不安全配置，可以在Cisco IOS XE 26.1.1及更高版本上使用show system insecure configuration命令。此命令提供设备上配置的限制阶段不安全功能的综合列表。此外，在Cisco SD-WAN Manager中，您可以导航到Monitor > Advisories并选择Insecure Configurations选项卡，以查看设备、配置组和模板间的不安全配置，以及补救步骤链接。此视图大约每30分钟刷新一次，以确保获得最新信息。

问:如何查看给定软件版本上所有可能的不安全配置的列表？

A：您可以使用命令show system insecure profile查看系统要检测的所有Restriction-phase insecure CLI模式的完整列表。与show system insecure configuration（仅显示当前应用的不安全配置）不同，配置文件输出在限制阶段包括所有已知的不安全配置，并随着安全最佳实践的发展而不断更新。

问:我纠正了一个不安全的配置。 为什么它仍然显示在show system insecure配置输出中？

答：不安全的配置的扫描仅在处于不安全的模式下定期运行。这意味着在更正不安全的配置后，系统无法立即反映更改，直到进行下一次计划扫描（30分钟间隔）。此计划可确保定期更新和显示最新的不安全配置详细信息，同时最大限度地减少执行扫描所需的开销。 您可以使用test system secure all命令强制立即重新扫描，这样您就不必等待扫描计时器过期。

问:如何在升级之前主动检查已应用的不安全配置？

答：要主动检查您在升级之前应用了哪些不安全配置，在Cisco IOS XE 17.18.2之前，客户可以使用Cisco Resilient Infrastructure页面上提供的Cisco AI Assistant for Support bot，该页面允许上传配置以识别不安全功能。类似工具，Cisco Config Resilient Infrastructure Tester是客户的另一个选择。 从Cisco IOS XE 17.18.2及更高版本开始，客户仍然可以使用这些工具，但您也可以在您的设备上直接运行命令show system insecure configuration，以查看当前应用的不安全配置。但是，使用AI Assistant for Support bot和Resilient Infrastructure Tester提供除直接CLI命令之外的其他AI驱动的扩充。

其它资源

我们鼓励客户通读此文档，以补充对其安全最佳实践和现有不安全配置的替代方案的了解。

思科弹性基础设施 — 提供跨思科设备向增强安全状态过渡的基本背景，用户可利用此页右下角的Cisco AI Assistant for Support Bot逐步执行指导式工作流程，从各种输出中识别不安全的配置

Cisco Config Resilient Infrastructure Tester — 可用于根据提供的运行配置检查不安全的配置的工具

Cisco IOS XE软件加固指南 — 详细介绍强化Cisco IOS XE设备并提高网络整体安全性的最佳实践

功能删除和建议备选方案 — 记录计划最终删除的不安全功能和协议以及建议替代方案的列表

功能弃用和删除详细信息 — 记录特定不安全的功能和协议何时进入基于Cisco IOS XE软件版本的警告和/或限制阶段

SD-WAN Monitor and Maintain Guide - Insecure Configuration Management章 — 涵盖对Cisco Catalyst SD-WAN中不安全的功能配置的集中式可视性和可行的补救，可帮助管理员识别和修复漏洞，从而增强网络安全性并保持合规性

可恢复的基础设施：Cisco Catalyst SD-WAN和路由技术参考 — Cisco Catalyst SD-WAN和路由的安全加固和恢复能力手册。它提供规范性的指导，以跨基于CLI和UI的管理模式识别、修复和替换不安全的配置，旨在通过从不安全替代方案过渡到安全、弹性的替代方案，加强安全性、减少攻击面，并保护数据，同时确保运营模式的一致性

Cisco C9000交换Cisco IOS XE — 弹性基础设施手册 — 专注于识别不安全的配置，并使用安全、弹性的替代方案替换这些配置，以增强安全状态、减少攻击面，并保护数据。本攻略旨在确保CLI和UI操作模型的一致性，同时增强Catalyst 9000系列的网络恢复能力和操作简便性

思科9800无线弹性基础设施 — 概述思科分阶段采取的策略，以淘汰不安全的功能和协议，提供全面的迁移路径以保护替代方案，防止软件升级期间服务中断。它包括详细的参考表，用于跨行传输、文件传输和管理协议进行受影响的配置，并包括未能迁移的潜在操作影响的指导

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。