Verstehen einer ausfallsicheren Infrastruktur auf IOS XE-Geräten

Inhalt

Einleitung

In diesem Dokument wird der Ansatz von Cisco für eine ausfallsichere Infrastruktur beschrieben, dessen Ursprung in der standardmäßigen und der standardmäßigen Sicherheit liegt.

Voraussetzungen

Anforderungen

Obwohl dieses Dokument keine spezifischen Anforderungen enthält, sind grundlegende Kenntnisse der Cisco IOS ® XE Software äußerst hilfreich.

Verwendete Komponenten

Die Informationen in diesem Dokument gelten für alle Geräte, auf denen Cisco IOS XE 17.18.2 oder höher ausgeführt werden kann. Dazu gehören Cisco IOS XE Router, Switches und WLCs.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Ziel

Unser Ziel ist es, die Angriffsfläche auf Netzwerkprodukte von Cisco deutlich zu verringern und Sicherheitslücken durch sichere Standardeinstellungen, das Entfernen unsicherer älterer Technologien und Funktionen und eine verbesserte Produktsicherheit zu minimieren.

Weitere Informationen zur Verbesserung der Netzwerksicherheit bei Cisco finden Sie in der Dokumentation zur ausfallsicheren Infrastruktur sowie im Cisco IOS XE Software Hardening Guide. In diesem Dokument werden jedoch in erster Linie die technischen Aspekte und Überlegungen behandelt, die sich aus der schrittweisen Implementierung dieser wichtigen Sicherheitsänderungen ergeben.

Phasenweiser Ansatz

Um eine geringere Angriffsfläche und die Einführung wichtiger Best Practices für die Sicherheit zu gewährleisten und gleichzeitig Unterbrechungen und Aufwand für unsere Kunden zu minimieren, verfolgt Cisco einen schrittweisen Ansatz zur Beseitigung unsicherer Funktionen und Protokolle. Beachten Sie, dass das Phasing von unsicheren Konfigurationen funktionen- oder protokollspezifisch ist. Eine Funktion kann in der Warnphase verbleiben, während eine andere Funktion in die Beschränkungsphase eintritt.

Phase 1: Warnung

Benutzer erhalten Warnungen in der CLI, wenn sie wichtige unsichere Funktionen konfigurieren. Unser Ziel ist es, Kunden auf diese unsicheren Konfigurationen aufmerksam zu machen, damit sie mit der Migration zu sichereren Optionen beginnen können. Cisco empfiehlt dringend, alle unsicheren Warnmeldungen sofort zu beheben. Unsichere Konfigurationen in der Warnphase lösen den ungesicherten Modus nicht aus oder erfordern diesen.

Cisco IOS XE Version 17.18.2 ist die erste Softwareversion, die die Warnphase bei unsicheren Funktionen einführt.

Phase 2: Einschränkung

Wichtige unsichere Funktionen sind standardmäßig deaktiviert und erfordern eine explizite Benutzeraktion zur Aktivierung (durch Einführung des unsicheren Modus). Bestehende Bereitstellungen funktionieren weiterhin, neue Installationen erfordern jedoch die absichtliche Aktivierung dieser unsicheren Konfigurationen. Beachten Sie, dass einige Funktionen auf Cisco IOS XE-Plattformen nicht eingeschränkt werden können: können

einfach Warnungen für mehrere Releases anzeigen, bevor sie wieder entfernt werden.

Cisco IOS XE Version 26.1.1 ist die erste Softwareversion, die die Beschränkungsphase für unsichere Funktionen einführt.

Phase 3: Entfernen

Veraltete, unsichere Funktionen werden vollständig entfernt. Der Zeitpunkt des Entfernens dieser Funktion ist von den Auswirkungen auf den Benutzer und von der Einführung abhängig. Weit verbreitete Funktionen wie SNMPv2 sollen beispielsweise langsamer auslaufen als weniger häufig verwendete.

Cisco IOS XE Version 26.2.1 ist die erste Softwareversion, die die Deinstallationsphase für unsichere Funktionen vorstellt.

Wichtige Befehle

Diese Befehle sind äußerst nützlich, wenn Kunden eine ausfallsicherere Infrastruktur implementieren. Auf diese Befehle wird in diesem Dokument Bezug genommen.

- Unsichere Systemkonfiguration anzeigen
    - Mit diesem Befehl werden die aktuell angewendeten, unsicheren Konfigurationen angezeigt, die sich in der Einschränkungsphase befinden. Es werden keine unsicheren Konfigurationen angezeigt, die sich in der Warn- oder Deinstallationsphase befinden. Mit diesem Befehl wird auch die verbleibende Zeit für die nächste Suche nach unsicheren Konfigurationen angezeigt (weitere Informationen finden Sie im Abschnitt Timers and Insecure Configuration Scans (Timer- und unsichere Konfigurationsscans)).
- Anzeigen des Systemsicherheitsmodus
    - Dieser Befehl zeigt in einer kurzen Ausgabe an, ob sich das Gerät im abgesicherten Modus oder im ungesicherten Modus befindet.
- show running-config all | Systemmodus unsicher einschließen
    - Dieser Befehl zeigt die aktuelle Konfiguration (einschließlich der Standardkonfigurationen) an, die nach den Schlüsselwörtern für den Systemmodus "unsicher" gefiltert wurde. Weitere Informationen finden Sie im Abschnitt "Sicherheitsmodus ändern".
- Prüfsystem sichern alle
    - Mit diesem Befehl wird sofort eine Suche nach unsicheren Konfigurationen durchgeführt und die Ausgabe von show system insecure configuration angezeigt. Dies ist hilfreich, um die Konfigurationen mit unsicheren Kennzeichnungen nach einer Änderung zu aktualisieren, ohne darauf zu warten, dass der Scan-Timer abläuft.
- Unsicheres Systemprofil anzeigen
    - Dieser Befehl zeigt unsichere Konfigurationen in der Restriction-Phase an, die das System auf dieser Softwareversion erkennen soll. Die Liste der unsicheren Konfigurationen im Profil wird mit der Zeit aktualisiert, da die Best Practices für die Sicherheit ständig weiterentwickelt werden. Dies spiegelt nicht die unsicheren Funktionen wider, die derzeit auf dem Gerät konfiguriert sind. Es handelt sich lediglich um eine Liste aller unsicheren Konfigurationen der Restriction-Phase, die vom System erkannt werden. Informationen zu allen Best Practices für die Sicherheit finden Sie in den Härtungsleitfäden im Abschnitt "Zusätzliche Ressourcen".

Hinweise und Überlegungen

Timer und Scans nach unsicheren Konfigurationen

Die in diesem Dokument beschriebenen unsicheren Konfigurationsprüfungen und Warnmeldungen werden für Zeitgeber eingeplant, um die Häufigkeit ihrer Ausführung zu begrenzen. Wenn eine unsichere Konfiguration korrigiert wird, wird sie nicht sofort aus der Ausgabe von show system insecure configuration (Systemunsichere Konfiguration anzeigen) entfernt. Der Konfigurationsscanner arbeitet mit einem 30-minütigen Zyklus und hat eine

Verzögerung von bis zu 30 Minuten. Ebenso kann es zu einer Verzögerung von bis zu zwei Minuten zwischen dem Anwenden einer unsicheren Konfiguration und dem entsprechenden %SYS-4-INSECURE_CONFIG-Syslog kommen.

Mit dem Befehl show system insecure configuration (Unsicheres System anzeigen) können Benutzer die verbleibende Zeit bis zum nächsten Scan anzeigen. Der Timer wird im ersten Ausgabeteil angezeigt. Das erste Beispiel zeigt, dass Konfigurationsänderungen vorgenommen wurden und die nächste Suche nach unsicheren Konfigurationen in 8 Minuten erfolgt:

```
<#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>
```

Das folgende Beispiel zeigt, dass seit dem letzten Scan keine Konfigurationsänderungen erkannt wurden, sodass keine weiteren Prüfungen auf unsichere Konfigurationen erforderlich sind:

```
<#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>
```

Benutzer können eine sofortige erneute Suche erzwingen, indem sie den Befehl secure all des Testsystems verwenden. Zusätzlich zum sofortigen erneuten Scannen zeigt dieser Befehl die Ausgabe von show system insecure configuration an. Dies ist hilfreich, um die Konfigurationen mit der Kennzeichnung "unsecure" nach einer Änderung zu aktualisieren, ohne darauf zu warten, dass der Scan-Timer abläuft.

Warnungen zu unsicheren Konfigurationen

Ab Version 17.18.2 mit der Einführung der Warnphase wird die folgende Syslog-Syntax angezeigt:

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

Zu diesen Meldungen gehören:

- Modul: Die Komponente, die die Protokollmeldung generiert hat (z. B. LOGGING, HTTP oder LINE)
- Command: Die spezifische Konfiguration, die die Warnmeldung ausgelöst hat
- Grund: Der Grund, warum diese Konfiguration als unsicher gekennzeichnet wird
- Problembehebung: Maßnahmen zur Migration auf eine sicherere Alternative

Diese Warnmeldungen wirken sich nicht auf den Dienst oder die Funktionalität auf dem Gerät aus. Ziel ist es, die Aufmerksamkeit auf diese unsicheren Konfigurationen zu lenken, damit sie vom Benutzer proaktiv gemindert werden können.

Anmerkung: Ab Cisco IOS XE Version 26.1.1 weisen die INSECURE_DYNAMIC_WARNING-Meldungen auf unsichere Konfigurationen in der Warnphase hin, während die INSECURE_CONFIG-Meldungen auf unsichere Konfigurationen in der Einschränkungsphase hinweisen. In der Ausgabe von show system insecure configuration werden nur eingeschränkte Konfigurationen angezeigt.

Beachten Sie, dass diese Protokolle beim Hochfahren oder nach Anwenden einer unsicheren Konfiguration angezeigt werden. Darüber hinaus können sie periodisch wieder auf dem Gerät erscheinen. Weitere Details zu diesen Meldungen und ihrer Syntax finden Sie in der Cisco IOS

XE Security Warnings Reference (Cisco IOS XE-Sicherheitshinweise für ausfallsichere Infrastruktur).

Syslog-Beispielerkennung kurz nach der Konfiguration

Dies sind Beispiel-Syslog-Meldungen, die kurz nach der Anwendung einer unsicheren Konfiguration angezeigt werden. Wie im Abschnitt Scans mit Timern und unsicheren Konfigurationen beschrieben, kann es nach Anwendung der unsicheren Konfiguration bis zu zwei Minuten dauern, bis diese Meldungen angezeigt werden:

```
! 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
```

Syslog-Beispiel beim Systemstart

Dies sind Beispielmeldungen, die beim Systemstart angezeigt werden. Für jede vom System erkannte unsichere Konfiguration wird eine Meldung angezeigt:

```
! 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
```

Unsicherer Modus

Der unsichere Modus wird mit Cisco IOS XE Version 26.1.1 eingeführt. Der Insecure Mode soll dabei helfen, die Lücke zwischen bestehenden, unsicheren Bereitstellungen und zukünftigen, robusten Netzwerken zu schließen. Durch Hinzufügen der Konfiguration des unsicheren Modus können Kunden weiterhin mit vorhandenen, unsicheren Funktionen arbeiten und gleichzeitig angeben, welche Konfigurationen ein Sicherheitsrisiko darstellen und reduziert werden müssen. Sie dient außerdem als Quittung für unsichere Funktionen, bevor diese auf ein werkseitig voreingestelltes Gerät angewendet werden. Der ungesicherte Modus ermöglicht außerdem die Planung des End-of-Life-Zeitraums für veraltete Funktionen, bevor diese in Phase 3 vollständig entfernt werden. Ziel des "Insecure Mode" ist es, Kunden auf sichere Netzwerke zu migrieren und gleichzeitig potenzielle Funktionsstörungen zu minimieren.

Für neue Bereitstellungen und Neuinstallationen, die werksseitig standardmäßig eingestellt sind, ist der abgesicherte Modus standardmäßig eingestellt (kein unsicherer Systemmodus), d. h., das Gerät erlaubt Benutzern nicht, unsichere Konfigurationen in der Restriction-Phase anzuwenden. Benutzer müssen den unsicheren Modus explizit mit der globalen Konfiguration für den unsicheren Systemmodus aktivieren, um unsichere Funktionen und Protokolle der Einschränkungsphase anzuwenden. Unsichere Funktionen und Protokolle in der Warnphase können weiterhin im abgesicherten Modus angewendet werden, sie generieren jedoch Warnmeldungen.

Aktuellen Sicherheitsmodus überprüfen

Benutzer können mit dem Befehl show system security mode (Systemsicherheitsmodus anzeigen) überprüfen, ob sich das Gerät im abgesicherten Modus oder im ungesicherten Modus befindet. Die Option show running-config all Der Befehl | include system mode gibt auch an, ob sich das Gerät im abgesicherten Modus oder im ungesicherten Modus befindet. Das Schlüsselwort all weist das Gerät an, Standardkonfigurationen in die Ausgabe aufzunehmen, da der abgesicherte Modus die Standardeinstellung für neue Bereitstellungen ist.

Diese Ausgaben spiegeln ein Gerät im abgesicherten Modus wider:

<#root>

```
Device#

show system security mode


System Security Mode :

Secure



Device#

show running-config all | include system mode



no system mode insecure
```

Mit den gleichen Befehlen kann überprüft werden, ob sich das Gerät im ungesicherten Modus befindet:

<#root>

```
Device#

show system security mode


System Security Mode :

Insecure



Device#

show running-config all | include system mode



system mode insecure
```

Sicherheitsmodus ändern

Unsicheren Modus aktivieren

Benutzer können den ungesicherten Modus mit der globalen Konfiguration für den ungesicherten Systemmodus aktivieren:

<#root>

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

system mode insecure
```

Sicheren Modus aktivieren

Benutzer können den abgesicherten Modus aktivieren, wenn die globale Konfiguration keinen Systemmodus enthält:

<#root>

```
Device# configure terminal
```

```
Device(config)#

no system mode insecure
```

Anforderungen zur Aktivierung des abgesicherten Modus

So wechseln Sie in den sicheren Modus:

- Alle unsicheren Konfigurationsüberprüfungen müssen abgeschlossen sein.
- Alle unsicheren Konfigurationen müssen vom Gerät entfernt werden.

Wenn der Scan der unsicheren Konfiguration nicht abgeschlossen ist, fordert das System den Benutzer auf, den Vorgang nach Ablauf des Scan-Timers erneut zu versuchen:

<#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.
```

Benutzer können eine sofortige erneute Suche erzwingen, indem sie den Befehl secure all des Testsystems verwenden.

Wenn das System nach Ablauf des Zeitgebers und Abschluss der Konfigurationsprüfung noch immer unsichere Konfigurationen erkennt, wechselt das System nicht in den abgesicherten Modus. Diese unsicheren Konfigurationen müssen entfernt werden, bevor das System in den abgesicherten Modus wechseln kann:

<#root>

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

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

Wenn beide Anforderungen erfüllt sind, können Benutzer den abgesicherten Modus aktivieren:

<#root>

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

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

Unsichere Konfigurationen anwenden

Wenn ein Benutzer im abgesicherten Modus versucht, eine nicht abgesicherte Konfiguration mit eingeschränkter Phase anzuwenden, wird eine Fehlermeldung angezeigt, und die Konfiguration wird nicht angewendet. Beispiele:

<#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
```

Die Meldungen, die unmittelbar nach dem Konfigurationsversuch angezeigt werden, weisen darauf hin, dass sich das Gerät im abgesicherten Modus befindet, sodass die bereitgestellten unsicheren Konfigurationen nicht angewendet werden können. Sie können bestätigen, dass die unsicheren Konfigurationen nicht angewendet wurden:

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

Um unsichere Konfigurationen für die Restriction-Phase anzuwenden, müssen die Benutzer zuerst explizit den unsicheren Modus mit der globalen Konfiguration für den unsicheren Systemmodus

aktivieren:

<#root>

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

system mode insecure


Device(config)# end

Device#show running-config all | include system mode

system mode insecure
```

Sobald sich das Gerät im ungesicherten Modus befindet, können die ungesicherten Konfigurationen der Restriction-Phase angewendet werden. Eine ähnliche Sicherheitswarnung wird bei der Konfiguration angezeigt. Die unsichere Konfiguration wird jedoch angewendet:

<#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#
```

Benutzer sehen außerdem eine Warnmeldung, die sie auf die unsichere Konfiguration aufmerksam macht. Da diese Meldungen von Timern in die Warteschlange gestellt werden, um sie einzuschränken, kann es nach der Konfiguration bis zu zwei Minuten dauern, bis dieses Syslog angezeigt wird:

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

Beachten Sie, dass nur Funktionen und Protokolle in der Einschränkungsphase den unsicheren Modus benötigen oder auslösen. Funktionen und Protokolle, die sich in der Warnphase befinden,

können weiterhin im abgesicherten Modus angewendet werden.

Automatischer Übergang in den ungesicherten Modus

Wenn ein Cisco IOS XE-Gerät auf 26.1.1 oder höher aktualisiert wird, erkennt das System während des Bootvorgangs unsichere Konfigurationen in der Restriction-Phase und wechselt das Gerät automatisch in den Unsicheren Modus. Die Benutzer müssen sich nicht darum kümmern, die globale unsichere Konfiguration des Systemmodus manuell hinzuzufügen, und beim Übergang zur Einschränkungsphase haben unsichere Funktionen keine Auswirkungen.

In diesem Beispiel wird der automatische Übergang zum ungesicherten Modus während des Upgrades von 17.18.2 (ohne Kontext des ungesicherten Modus) auf 26.1.1 (mit explizitem Kontext des ungesicherten Modus) durchlaufen. Das Gerät beginnt mit der angewendeten Konfiguration der unsicheren IP-FTP-Quellschnittstelle "GigabitEthernet0/0/0".

Dieses Gerät startet am Anfang auf Cisco IOS XE Version 17.18.2:

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

Es wurde eine unsichere Konfiguration erkannt:

<#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>
```

Darüber hinaus gibt es in dieser Version keine Konzepte für den abgesicherten oder nicht abgesicherten Modus:

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

Das Gerät wird dann auf 26.1.1 aktualisiert, wodurch der sichere und der unsichere Modus eingeführt wird.

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

Es wird immer noch die gleiche unsichere Konfiguration angewendet:

<#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>
```

Aufgrund dieser (oder einer) unsicheren Konfiguration in der Restriction-Phase erkennt das System automatisch den unsicheren Modus und wechselt in diesen:

<#root>

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

Insecure
```

Die Konfiguration für den unsicheren Systemmodus wird automatisch angewendet:

<#root>

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

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


system mode warning periodicity 24
Device#
```

Bitte beachten Sie, dass das Vorhandensein unsicherer Warnphasen-Konfigurationen keinen Übergang in den unsicheren Modus auslöst. Nur das Vorhandensein unsicherer Konfigurationen in der Restriction-Phase löst den automatischen Übergang aus.

Sicherung von Geräten

Es wird dringend empfohlen, vor der Phase der Deinstallation (Phase 3) alle Anstrengungen zu

unternehmen, um von unsicheren Funktionen und Protokollen auf sicherere Methoden umzusteigen. Cisco hat einige Verbesserungen der Benutzerfreundlichkeit integriert, um das Erkennen unsicherer Konfigurationen und deren Korrektur zu erleichtern.

Angewendete unsichere Konfigurationen identifizieren

Benutzer können unsichere Konfigurationen in der Einschränkungsphase anzeigen, die derzeit mit dem EXEC-Befehl show system insecure configuration angewendet werden. Dieser Befehl ist automatisch in der Ausgabe von show tech-support in Version 26.1.1 und höher enthalten. Dies ist ein Beispiel, das von einem Gerät ausgegeben wird, auf das drei unsichere Konfigurationen in der Einschränkungsphase angewendet wurden:

<#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>
```

Diese Ausgabe enthält wichtige Informationen zu dem Modul, das die unsichere Funktion enthält, zum übergeordneten Befehl oder zur Konfiguration, wenn es sich um eine geschachtelte Konfiguration handelt, zum markierten CLI-Befehl, zum Grund für die Markierung "unsicher" und zu den erforderlichen Korrekturmaßnahmen.

Benutzer können auch eine umfassende Liste aller unsicheren CLI-Muster anzeigen, indem sie den Befehl show system insecure profile verwenden. Während "Unsichere Konfiguration des Systems anzeigen" die aktuell angewendeten unsicheren Konfigurationen der Restriction-Phase anzeigt, zeigt "Unsicheres Profil des Systems anzeigen" alle unsicheren Konfigurationen der Restriction-Phase an, die das System erkennen soll. Die Liste der unsicheren Konfigurationen im Profil wird mit der Zeit aktualisiert, da die Best Practices für die Sicherheit ständig weiterentwickelt werden.

Beispiele zur Behebung häufig auftretender unsicherer Konfigurationen

Diese Beispiele zeigen, wie Benutzer mehrere häufig auftretende unsichere Konfigurationen erkennen, identifizieren und beheben können. Cisco hat Software implementiert, die die Identifizierung und Eindämmung von Bedrohungen so einfach wie möglich macht, unabhängig davon, ob die Benutzer die INSECURE_CONFIG-Syslog-Meldungen verwenden oder die unsichere Konfiguration des Systems anzeigen.

Unsichere Dateiübertragungsmethode

Folgende Warnmeldungen werden auf dem Gerät angezeigt:

```
%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
```

Sie können show system insecure configuration ausführen, um weitere Informationen zu diesen unsicheren Konfigurationen anzuzeigen:

<#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#
```

Diese Protokolle werden den folgenden Konfigurationen direkt zugeordnet:

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

Benutzer können die unsicheren Konfigurationen durch folgende Änderungen beheben:

<#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
```

Unsichere, ältere SNMP-Protokolle

Dies ist die Warnmeldung, die auf dem Gerät angezeigt wird:

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

Sie können show system insecure configuration ausführen, um weitere Informationen über die unsichere Konfiguration anzuzeigen:

<#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#
```

Diese Protokolle werden dieser Konfiguration direkt zugeordnet:

<#root>

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

snmp-server community

      RO
```

Kunden können dies mit SNMPv3 mit Authentifizierung und Verschlüsselung (authPriv) beheben.

Häufig gestellte Fragen

F: Warum nimmt Cisco diese Änderungen vor?

A: Cisco verbessert mit diesen Änderungen die Sicherheit und Ausfallsicherheit seiner Netzwerkinfrastruktur, indem es unsichere ältere Funktionen deaktiviert, stärkere Schutz- und Überwachungsfunktionen einführt und sichere Betriebsabläufe vereinfacht. So schützen wir unsere Kunden vor neuen Cyber-Bedrohungen, reduzieren Ausfallzeiten und bereiten unsere Netzwerke auf zukünftige Herausforderungen wie das Quantencomputing vor. Insgesamt zielt die Initiative darauf ab, eine moderne, sichere und zuverlässige Grundlage für aktuelle und zukünftige Technologien zu schaffen

F: Was passiert, wenn ein Gerät mit einer unsicheren Konfiguration in der Einschränkungsphase auf eine Version für diese Funktion aktualisiert wird?

A : Wenn ein Gerät für eine bestimmte Funktion auf eine eingeschränkte Version (Phase 2) aktualisiert wird, erkennt das System die unsicheren Konfigurationen während des Bootvorgangs und wechselt das Gerät automatisch in den ungesicherten Modus.

F: Was passiert, wenn ein Gerät mit einer unsicheren Konfiguration in der Phase zum Entfernen auf eine Version für diese Funktion aktualisiert wird?

A : Wenn für ein Gerät ein Upgrade auf eine Release zur Deinstallation (Phase 3) für eine

bestimmte Funktion durchgeführt wird, sind entfernte Konfigurationen nicht mehr verfügbar. Benutzer müssen zur Verwaltung veralteter Befehle Standardmigrationsverfahren einhalten.

F: Wurden alle unsicheren Funktionen in derselben Version entfernt?

A: Nicht alle unsicheren Funktionen werden in derselben Version entfernt. Cisco verfolgt einen schrittweisen Ansatz zur Beseitigung unsicherer Funktionen in drei Phasen: zunächst Warnungen ausgeben, wenn unsichere Funktionen konfiguriert oder erkannt werden, dann deren Verwendung einschränken, indem sie standardmäßig deaktiviert werden oder explizite Administratoraktionen erforderlich sind (durch Einführung des unsicheren Modus), und schließlich die Funktionen in zukünftigen Versionen vollständig entfernen. Einige Funktionen können die Restriction-Phase überspringen und direkt von Warnungen zu Deinstallation wechseln. Der Zeitpunkt der Deinstallation ist je nach Funktion und Plattform unterschiedlich. Die Versionsnummern für Warnungen, Einschränkungen und Deinstallationen variieren je nach Betriebssystem wie Cisco IOS XE, Cisco IOS XR, Cisco NXOS, Cisco ISE und Cisco ASA/FTD. Dieser mehrstufige Prozess gewährleistet minimale Unterbrechungen und lässt dem Kunden Zeit, auf sichere Alternativen umzusteigen.

F: Wann wird meine unsichere Funktion in die Beschränkungs- oder Entfernungsphase verschoben?

A: Der Zeitpunkt, zu dem das unsichere Feature in die Beschränkungs- oder Entfernungsphase übergeht, hängt von der Funktion und dem Betriebssystem ab. Ausführliche Informationen finden Sie in der Dokumentation zu Funktionseinbußen und -entfernungen.

F: Welche Alternativen gibt es für meine spezielle unsichere Funktion?

A : Kunden können in der Dokumentation zum Entfernen von Funktionen und vorgeschlagenen Alternativen nach empfohlenen Alternativen zu verschiedenen unsicheren Funktionen und Protokollen suchen.

F: Wie kann ich sehen, welche unsicheren Konfigurationen ich derzeit angewendet habe?

A: Mit dem Befehl show system insecure configuration auf Cisco IOS XE 26.1.1 und höheren Versionen können Sie sehen, welche unsicheren Konfigurationen in der Restriction-Phase aktuell angewendet wurden. Dieser Befehl stellt eine umfassende Liste der auf dem Gerät konfigurierten nicht sicheren Funktionen der Restriction-Phase bereit. Darüber hinaus können Sie im Cisco SD-WAN Manager zu Monitor > Advisories navigieren und die Registerkarte Insecure Configurations (Unsichere Konfigurationen) auswählen, um unsichere Konfigurationen auf allen Geräten, Konfigurationsgruppen und Vorlagen anzuzeigen, einschließlich Links zu Behebungsschritten. Diese Ansicht wird ca. alle 30 Minuten aktualisiert, um die aktuellsten Informationen zu erhalten.

F: Wie kann ich eine Liste aller möglichen unsicheren Konfigurationen einer bestimmten Softwareversion anzeigen?

A : Mit dem Befehl show system insecure profile können Sie eine vollständige Liste aller unsicheren CLI-Muster anzeigen, die das System erkennen soll. Im Gegensatz zur Anzeige einer unsicheren Konfiguration, die nur die aktuell angewendeten unsicheren Konfigurationen anzeigt, umfasst die Profilausgabe alle bekannten unsicheren Konfigurationen in der Einschränkungsphase und wird mit der Zeit aktualisiert, wenn die Sicherheitsvorkehrungen erweitert werden.

F: Ich habe eine unsichere Konfiguration korrigiert. Warum wird sie immer noch in der Ausgabe von show system insecure configuration angezeigt?

A: Die Suche nach unsicheren Konfigurationen wird nur in regelmäßigen Abständen im ungesicherten Modus ausgeführt. Das bedeutet, dass das System nach der Korrektur einer unsicheren Konfiguration die Änderung nicht sofort wiedergeben kann, bis der nächste geplante Scan stattfindet, der in einem Intervall von 30 Minuten erfolgt. Durch diese Planung wird sichergestellt, dass die neuesten unsicheren Konfigurationsdetails regelmäßig aktualisiert und angezeigt werden. Gleichzeitig wird der für die Suche erforderliche Overhead minimiert. Sie können den Befehl secure all des Testsystems verwenden, um eine sofortige erneute Suche zu erzwingen, sodass Sie nicht warten müssen, bis der Scan-Timer abläuft.

F: Wie kann ich vor dem Upgrade proaktiv prüfen, welche unsicheren Konfigurationen ich angewendet habe?

A: Um vor dem Upgrade auf Cisco IOS XE 17.18.2 proaktiv zu überprüfen, welche unsicheren Konfigurationen angewendet wurden, können Kunden den Cisco AI Assistant for Support verwenden, der auf der Seite für die ausfallsichere Infrastruktur von Cisco verfügbar ist. Auf diese Weise können Sie Konfigurationen hochladen, um unsichere Funktionen zu identifizieren. Ein ähnliches Tool, der Cisco Config Resilient Infrastructure Tester, ist eine weitere Option für Kunden. Ab Cisco IOS XE 17.18.2 können Kunden diese Tools weiterhin verwenden. Sie haben jedoch auch die Möglichkeit, den Befehl show system insecure configuration direkt auf Ihren Geräten auszuführen, um die aktuell angewendeten unsicheren Konfigurationen anzuzeigen. Der AI Assistant for Support-Bot und der Resilient Infrastructure Tester bieten jedoch zusätzlich zum direkten CLI-Befehl eine KI-gesteuerte Erweiterung.

Zusätzliche Ressourcen

Es wird empfohlen, diese Dokumentation zu lesen, um das Verständnis von Best Practices und Alternativen zu bestehenden, unsicheren Konfigurationen zu vertiefen.

Ausfallsichere Cisco Infrastruktur - Stellt wichtige Hintergrundinformationen zum Übergang zu einem verbesserten Sicherheitsstatus für Cisco Geräte bereit, und Benutzer können den Cisco AI Assistant for Support Bot in der rechten unteren Ecke dieser Seite nutzen, um einen geführten Workflow zu durchlaufen und unsichere Konfigurationen aus verschiedenen Ausgaben zu identifizieren.

Cisco Config Resilient Infrastructure Tester: Tool zur Überprüfung auf unsichere Konfigurationen anhand der bereitgestellten Ausführungskonfiguration

Cisco IOS XE Software Hardening Guide: Hier finden Sie Best Practices zum Schutz Ihrer Cisco IOS XE-Geräte und zur Erhöhung der allgemeinen Netzwerksicherheit.

Entfernen von Funktionen und empfohlene Alternativen - Dokumentiert die Liste der unsicheren Funktionen und Protokolle, die für eine spätere Entfernung geplant sind, sowie die empfohlenen Alternativen

Details zu Funktionseinschränkungen und -entfernungen - Dokumentiert, wenn bestimmte unsichere Funktionen und Protokolle in Warn- und/oder Beschränkungsphasen eintreten, basierend auf der Cisco IOS XE-Softwareversion

Leitfaden zu Überwachung und Wartung des SD-WAN - Kapitel zum Management unsicherer Konfigurationen - Umfasst zentrale Transparenz und umsetzbare Maßnahmen zur Behebung unsicherer Funktionskonfigurationen im Cisco Catalyst SD-WAN. Administratoren können Schwachstellen identifizieren und beheben, um die Netzwerksicherheit zu erhöhen und die Compliance zu gewährleisten

Ausfallsichere Infrastruktur: Technische Referenz zu Cisco Catalyst SD-WAN und Routing: Strategischer Leitfaden zur Erhöhung der Sicherheit und zur Erhöhung der Ausfallsicherheit für Cisco Catalyst SD-WAN und Routing. Sie bietet eine präskriptive Anleitung für die Erkennung, Behebung und den Austausch unsicherer Konfigurationen über CLI- und UI-basierte Managementmodelle hinweg. Ziel ist es, die Sicherheit zu erhöhen, die Angriffsfläche zu verringern und Daten zu schützen, indem von unsicheren zu sicheren, ausfallsicheren Alternativen übergegangen wird, während gleichzeitig die Konsistenz aller Betriebsmodelle gewährleistet wird.

Cisco C9000 Switching Cisco IOS XE - Strategischer Leitfaden für eine ausfallsichere Infrastruktur - Schwerpunkt auf der Identifizierung unsicherer Konfigurationen und deren Ersetzung durch sichere, ausfallsichere Alternativen, um den Sicherheitsstatus zu stärken, die Angriffsfläche zu verringern und Daten zu schützen. Der strategische Leitfaden zielt darauf ab, Konsistenz über alle CLI- und UI-Betriebsmodelle hinweg sicherzustellen und gleichzeitig die Ausfallsicherheit und den einfachen Betrieb des Netzwerks für die Catalyst Serie 9000 zu verbessern.

Cisco 9800 Wireless Resilient Infrastructure (Wireless-Ausfallsichere Infrastruktur) - beschreibt die

mehrstufige Strategie von Cisco für die Außerkraftsetzung unsicherer Funktionen und Protokolle und stellt umfassende Migrationspfade für sichere Alternativen bereit, um Serviceunterbrechungen während Software-Upgrades zu vermeiden. Es enthält detaillierte Referenztabellen zu den betroffenen Konfigurationen für den Line-Transport, Dateiübertragungen und Managementprotokolle sowie Hinweise zu den möglichen betrieblichen Auswirkungen einer nicht erfolgten Migration.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.