IOS XE 디바이스의 복원력 있는 인프라 이해

목차

소개

이 문서에서는 기본적으로 안전하고 설계에 따라 안전한 인프라를 기반으로 하는 Cisco의 복원력 있는 인프라에 대한 접근 방식을 설명합니다.

사전 요구 사항

요구 사항

이 문서에는 특별한 요구 사항이 없지만 Cisco IOS ® XE 소프트웨어에 대한 기본적인 이해가 매우 유용합니다.

사용되는 구성 요소

이 문서의 정보는 Cisco IOS XE 17.18.2 이상 소프트웨어를 실행할 수 있는 모든 장치에 적용됩니다. 여기에는 Cisco IOS XE 라우터, 스위치 및 WLC가 포함됩니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

목표

Cisco의 목표는 안전한 기본 설정, 안전하지 않은 레거시 기술 및 기능 제거, 향상된 제품 보안을 통해 Cisco 네트워킹 제품의 공격 표면을 의미 있게 줄이고 보안 취약점을 최소화하는 것입니다.

네트워크 보안 상태 개선을 위한 Cisco의 노력에 대한 자세한 내용은 Resilient Infrastructure 문서 및 Cisco IOS XE Software Hardening Guide를 참조하십시오. 그러나 이 문서에서는 주로 이러한 중요한 보안 변경의 단계적 구현으로 인한 기술적 측면 및 고려 사항에 중점을 둡니다.

단계별 접근 방식

Cisco는 공격 표면을 줄이고 중요한 보안 모범 사례를 채택하는 동시에 고객의 중단과 노력을 최소화하기 위해 보안되지 않은 기능과 프로토콜을 제거하는 단계적 접근 방식을 취하고 있습니다. 안전하지 않은 컨피그레이션의 단계는 기능별 또는 프로토콜별 단계입니다. 한 피쳐는 경고 단계에 있고 다른 피쳐는 제한 단계에 들어갈 수 있습니다.

1단계: 경고

사용자는 주요 비보안 기능을 구성할 때 CLI에서 경고를 받습니다. Cisco의 목표는 이러한 안전하

지 않은 컨피그레이션에 대한 인식을 높임으로써 고객이 더 안전한 옵션으로 마이그레이션하는 계획을 시작할 수 있도록 하는 것입니다. Cisco에서는 안전하지 않은 경고 메시지를 즉시 처리할 것을 적극 권장합니다. 경고 단계의 비보안 컨피그레이션은 비보안 모드를 트리거하거나 요구하지 않습니다.

Cisco IOS XE 버전 17.18.2는 안전하지 않은 기능에 대해 경고 단계를 도입한 최초의 소프트웨어 릴리스입니다.

2단계: 제한 사항

주요 비보안 기능은 기본적으로 비활성화되어 있으며, (비보안 모드의 도입을 통해) 활성화하려면 명시적인 사용자 작업이 필요합니다. 기존 구축은 계속 작동하지만, 새로운 설치를 위해서는 이러한 안전하지 않은 컨피그레이션을 의도적으로 활성화해야 합니다. Cisco IOS XE 플랫폼의 일부 기능에는 제한 단계가 포함될 수 없습니다. Cisco는

후속 제거 전에 여러 릴리스에 대한 경고를 표시하기만 하면 됩니다.

Cisco IOS XE 버전 26.1.1은 안전하지 않은 기능에 대한 제한 단계를 도입한 최초의 소프트웨어 릴리스입니다.

3단계: 제거

부적절하고 보안되지 않은 기능은 완전히 제거됩니다. 기능 제거 시기는 사용자의 영향과 채택 여부에 따라 달라집니다. 예를 들어, SNMPv2와 같이 널리 채택된 기능은 덜 일반적으로 사용되는 기능보다 더 느린 페이즈 아웃(phase out)이 가능합니다.

Cisco IOS XE 버전 26.2.1은 안전하지 않은 기능에 대한 제거 단계를 도입한 최초의 소프트웨어 릴리스입니다.

키 명령

이러한 명령은 고객이 더 복원력이 뛰어난 인프라를 구현할 때 매우 유용합니다. 이러한 명령은 이 문서 전체에서 참조됩니다.

- 시스템 비보안 컨피그레이션 표시
  - 이 명령은 제한 단계에 있는 현재 적용된 안전하지 않은 컨피그레이션을 표시하는 데 사용됩니다. 경고 단계 또는 제거 단계에 있는 비보안 컨피그레이션은 표시되지 않습니다

. 이 명령은 다음 비보안 컨피그레이션 스캔의 남은 시간도 표시합니다(타이머 및 비보안 컨피그레이션 스캔 섹션에 자세히 설명).

- 시스템 보안 모드 표시
  - 이 명령은 디바이스가 보안 모드인지 비보안 모드인지를 보여 주는 간단한 출력을 제공합니다.
- show running-config all | 안전하지 않은 시스템 모드 포함
  - 이 명령은 시스템 모드 insecure 키워드에서 필터링된 실행 중인 컨피그레이션(기본 컨피그레이션 포함)을 표시합니다. 자세한 내용은 보안 모드 변경 섹션을 참조하십시오.
- 테스트 시스템 보안 모두
  - 이 명령은 비보안 컨피그레이션 검사를 즉시 실행하고 show system insecure 컨피그레이션 출력을 표시합니다. 이렇게 하면 스캔 타이머가 만료될 때까지 기다리지 않고 변경 후 비보안 플래그가 지정된 컨피그레이션을 새로 고치는 데 유용합니다.
- 시스템 비보안 프로파일 표시
  - 이 명령은 시스템이 해당 버전의 소프트웨어에서 탐지하도록 설계된 제한 단계 비보안 컨피그레이션을 표시합니다. 보안 모범 사례가 계속 발전함에 따라 프로필의 안전하지 않은 컨피그레이션 목록이 시간이 지남에 따라 업데이트됩니다. 이는 디바이스에 현재 구성된 비보안 기능을 반영하지 않습니다. 이는 시스템이 탐지하는 모든 제한 단계 비보안 컨피그레이션의 목록입니다. 모든 모범 보안 사례는 추가 리소스 섹션의 강화 가이드를 참조하십시오.

주의 사항 및 고려 사항

타이머 및 안전하지 않은 컨피그레이션 검사

이 문서 전반에서 자세히 설명된 안전하지 않은 컨피그레이션 확인 및 경고 메시지는 타이머의 실행 빈도를 평가-제한하도록 예약되어 있습니다. 안전하지 않은 컨피그레이션을 수정하더라도 show system insecure 컨피그레이션 출력에서 즉시 사라지지 않습니다. 컨피그레이션 스캐너가 30분 주기로 작동하므로 최대 30분의 지연이 발생한다. 마찬가지로, 비보안 컨피그레이션을 적용하는 것과 해당 %SYS-4-INSECURE_CONFIG syslog 사이에 최대 2분 정도 지연될 수 있습니다.

사용자는 show system insecure configuration 명령을 사용하여 다음 스캔이 실행될 때까지 남아 있는 시간을 볼 수 있습니다. 타이머는 출력의 첫 번째 섹션에 표시됩니다. 이 첫 번째 예에서는 컨피그레이션이 변경되었으며 비보안 컨피그레이션에 대한 다음 검사가 8분 후에 수행됨을 보여 줍니다.

<#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>
```

다음 예에서는 마지막 스캔 이후 컨피그레이션 변경이 감지되지 않았으므로 안전하지 않은 컨피그레이션에 대한 추가 검사가 필요하지 않음을 보여 줍니다.

<#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>
```

사용자는 test system secure all 명령을 사용하여 즉시 다시 검색할 수 있습니다. 이 명령은 즉시 다시 스캔을 요청하는 것 외에도 show system insecure configuration 출력을 표시합니다. 스캔 타이머가 만료될 때까지 기다리지 않고 변경 후 비보안 플래그가 지정된 구성을 새로 고치는 데 유용합니다.

안전하지 않은 컨피그레이션 경고

17.18.2부터 Warning 단계가 도입되면 다음과 같은 syslog 구문이 표시됩니다.

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

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

이러한 메시지는 다음과 같습니다.

- 모듈: 로그 메시지를 생성한 구성 요소(예: LOGGING, HTTP 또는 LINE)
- 명령을 사용합니다: 경고 메시지를 트리거한 특정 구성
- 이유: 이 컨피그레이션이 안전하지 않은 것으로 플래그가 지정된 이유
- 교정: 보다 안전한 대안으로 마이그레이션하기 위해 필요한 조치

이러한 경고 메시지는 디바이스의 서비스 또는 기능에 영향을 주지 않습니다. 이러한 안전하지 않은 컨피그레이션을 사용자가 사전에 차단할 수 있도록 주의를 기울이는 것이 목적입니다.

참고: Cisco IOS XE 버전 26.1.1부터 INSECURE_DYNAMIC_WARNING 메시지는 경고 단계에서 안전하지 않은 컨피그레이션을 나타내며, INSECURE_CONFIG 메시지는 제한 단계에서 안전하지 않은 컨피그레이션을 나타냅니다. show system insecure 컨피그레이션 출력에는 제한 단계 컨피그레이션만 표시됩니다.

부팅 시 또는 안전하지 않은 컨피그레이션을 적용한 후에 이러한 로그가 표시된다는 점에 유의하십시오. 또한 주기적으로 디바이스에 다시 나타날 수 있습니다. 이러한 메시지와 해당 구문에 대한 자세한 내용은 Resilient Infrastructure Cisco IOS XE Security Warnings Reference(복원력 있는 인프라 Cisco IOS XE 보안 경고 참조)를 참조하십시오.

컨피그레이션 직후 확인된 Syslog 예

다음은 안전하지 않은 컨피그레이션을 적용한 직후에 표시되는 syslog 메시지의 예입니다. Timers and Insecure Configuration Scans(타이머 및 비보안 컨피그레이션 검사) 섹션에서 설명한 것처럼, 이러한 메시지는 비보안 컨피그레이션을 적용한 후 표시될 때까지 최대 2분이 소요될 수 있습니다.

```
! 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
```

부팅에 표시되는 Syslog 예

다음은 부팅에 표시되는 메시지의 예입니다. 시스템에서 탐지하는 각 비보안 컨피그레이션에 대해 다음과 같은 메시지가 표시됩니다.

```
! 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
```

비보안 모드

비보안 모드는 Cisco IOS XE 버전 26.1.1부터 도입되었습니다. 비보안 모드는 기존의 비보안 구축과 미래의 강화된 네트워크 사이의 간극을 메우는 데 도움이 됩니다. Insecure Mode 컨피그레이션이 추가됨에 따라 고객은 기존의 비보안 기능을 계속 사용하면서 어떤 컨피그레이션이 보안 위험을 야기하고 이를 완화해야 하는지 플래그할 수 있습니다. 또한 공장 기본 디바이스에 적용하기 전에 안전하지 않은 기능을 승인하는 역할을 합니다. 비보안 모드에서는 기능이 완전히 제거되는 3단계 이전에 더 이상 사용되지 않는 기능에 대한 단종 계획도 가능합니다. Insecure Mode의 목표는 고객이 설계별 보안 네트워크로 마이그레이션하는 동시에 기능의 잠재적 중단을 최소화하는 것입니다.

공장 기본값인 신규 구축 및 신규 설치의 경우 보안 모드가 기본적으로 설정됩니다(시스템 모드 비보안 없음). 즉, 디바이스에서 사용자가 제한 단계 비보안 컨피그레이션을 적용할 수 없습니다. 사용자는 제한 단계 비보안 기능 및 프로토콜을 적용하려면 시스템 모드 비보안 전역 컨피그레이션으로 비보안 모드를 명시적으로 활성화해야 합니다. Warning 단계의 비보안 기능 및 프로토콜은 보안 모드에서 계속 적용할 수 있지만 경고 메시지를 생성합니다.

현재 보안 모드 확인

사용자는 show system security mode 명령을 사용하여 디바이스가 보안 모드인지 비보안 모드인지 확인할 수 있습니다. show running-config all | include system mode 명령은 장치가 보안 모드인지 비보안 모드인지도 반영합니다. all 키워드는 새 배포에서 보안 모드가 기본 설정이므로 기본 구성을 출력에 포함하도록 장치에 지시합니다.

이러한 출력은 보안 모드의 디바이스를 반영합니다.

```
<#root>
Device#

show system security mode


System Security Mode :

Secure
```

```
Device#
```

show running-config all | include system mode

no system mode insecure

동일한 명령을 사용하여 디바이스가 비보안 모드에 있는지 확인할 수 있습니다.

<#root>

```
Device#
```

show system security mode

```
System Security Mode :
```

Insecure

```
Device#
```

show running-config all | include system mode

system mode insecure

보안 모드 변경

비보안 모드 활성화

사용자는 시스템 모드 비보안 전역 컨피그레이션으로 비보안 모드를 활성화할 수 있습니다.

<#root>

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

system mode insecure

보안 모드 활성화

사용자는 보안 글로벌 컨피그레이션에서 시스템 모드가 없는 보안 모드를 활성화할 수 있습니다.

<#root>

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

no system mode insecure

보안 모드를 활성화하기 위한 요구 사항

보안 모드로 전환하려면

- 안전하지 않은 컨피그레이션 검사를 완료해야 합니다.
- 안전하지 않은 모든 컨피그레이션은 디바이스에서 제거해야 합니다.

안전하지 않은 컨피그레이션 검사가 완료되지 않은 경우, 시스템은 검사 타이머가 만료된 후 사용자에게 다시 시도하라는 메시지를 표시합니다.

<#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.

사용자는 test system secure all 명령을 사용하여 즉시 다시 검색할 수 있습니다.

타이머가 만료되고 컨피그레이션 스캔이 완료된 후에도 시스템에서 비보안 컨피그레이션을 탐지하는 경우 시스템이 보안 모드로 전환되지 않습니다. 시스템에서 보안 모드를 시작하려면 먼저 이러한 안전하지 않은 컨피그레이션을 제거해야 합니다.

<#root>

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

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

이러한 요구 사항이 모두 충족되면 사용자는 보안 모드를 활성화할 수 있습니다.

<#root>

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

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

안전하지 않은 컨피그레이션 적용

보안 모드에서 사용자가 제한된 단계의 비보안 컨피그레이션을 적용하려고 하면 오류 메시지가 표시되고 컨피그레이션이 적용되지 않습니다. 예를 들면 다음과 같습니다.

<#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
```

컨피그레이션 시도 직후 표시되는 메시지에서는 디바이스가 보안 모드에 있으므로 제공된 비보안 컨피그레이션을 적용할 수 없습니다. 안전하지 않은 컨피그레이션이 적용되지 않았음을 확인할 수 있습니다.

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

제한 단계 비보안 컨피그레이션을 적용하려면 사용자는 먼저 시스템 모드 비보안 전역 컨피그레이션에서 명시적으로 비보안 모드를 활성화해야 합니다.

<#root>

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

system mode insecure


Device(config)# end

Device#show running-config all | include system mode

system mode insecure
```

디바이스가 비보안 모드에 있으면 제한 단계 비보안 컨피그레이션을 적용할 수 있습니다. 컨피그레이션 시 유사한 보안 경고 메시지가 표시됩니다. 그러나 안전하지 않은 컨피그레이션이 적용됩니다.

<#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#
```

또한 안전하지 않은 컨피그레이션에 대한 주의를 요구하는 경고 메시지가 표시됩니다. 타이머를 속도 제한하기 위해 이러한 메시지를 큐잉하는 타이머 때문에 이 syslog는 구성 후 표시되는 데 최대 2분이 걸릴 수 있습니다.

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

제한 단계의 기능과 프로토콜만 비보안 모드를 필요로 하거나 트리거합니다. 경고 단계에 있는 기능 및 프로토콜은 보안 모드에서 계속 적용할 수 있습니다

비보안 모드로 자동 전환

Cisco IOS XE 디바이스를 26.1.1 이상으로 업그레이드하면 시스템은 부팅 프로세스 중에 제한 단계의 비보안 컨피그레이션을 탐지하고 자동으로 디바이스를 비보안 모드로 전환합니다. 사용자는 시스템 모드 비보안 글로벌 컨피그레이션 자체를 수동으로 추가하는 것에 대해 걱정할 필요가 없으며, Restriction 단계로 이동할 때 비보안 기능에 영향을 주지 않습니다.

이 예에서는 17.18.2(비보안 모드 컨텍스트가 없음)에서 26.1.1(명시적 비보안 모드 컨텍스트가 있음)로 업그레이드하는 동안 비보안 모드로의 자동 전환을 진행합니다. 디바이스는 비보안 ip ftp 소스 인터페이스 GigabitEthernet0/0/0 컨피그레이션이 적용된 상태로 시작합니다.

처음에는 이 디바이스가 Cisco IOS XE 버전 17.18.2에서 시작됩니다.

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

탐지된 비보안 컨피그레이션이 하나 있습니다.

<#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>
```

또한 이 버전에는 보안 모드 또는 비보안 모드의 개념이 없습니다.

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

그런 다음 디바이스가 26.1.1로 업그레이드되어 보안 및 비보안 모드가 도입됩니다.

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

여전히 동일한 비보안 컨피그레이션이 적용되어 있습니다.

<#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>
```

이(또는 임의의) 제한 단계 비보안 컨피그레이션이 존재하므로 시스템은 다음을 탐지하고 자동으로 비보안 모드로 전환합니다.

```
<#root>

Device# show system security mode
System Security Mode :

Insecure
```

그리고 시스템 모드 비보안 컨피그레이션이 자동으로 적용됩니다.

```
<#root>

Device# show running-config all | include system mode

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


system mode warning periodicity 24
Device#
```

경고 단계의 비보안 컨피그레이션이 있다고 해서 비보안 모드로의 전환이 트리거되는 것은 아닙니다. 제한 단계의 비보안 컨피그레이션이 있을 때만 자동 전환이 트리거됩니다.

장치 강화

제거 단계(3단계) 전에 안전하지 않은 기능과 프로토콜을 보다 안전한 방법으로 마이그레이션하기 위해 모든 노력을 기울이는 것이 좋습니다. Cisco는 일부 향상된 서비스 기능을 통합하여 안전하지 않은 컨피그레이션을 식별하고 이를 훨씬 쉽게 수정할 수 있도록 했습니다.

적용된 비보안 컨피그레이션 식별

사용자는 show system insecure configuration EXEC 명령으로 현재 적용된 제한 단계 비보안 컨피그레이션을 볼 수 있습니다. 이 명령은 버전 26.1.1 이상의 show tech-support 출력에 자동으로 포함됩니다. 다음은 세 가지 제한 단계 비보안 컨피그레이션이 적용된 디바이스의 출력 예입니다.

<#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>
```

이 출력에는 비보안 기능이 포함된 모듈, 중첩된 컨피그레이션인 경우 상위 명령 또는 컨피그레이션, 플래그가 지정된 특정 CLI 명령, 비보안으로 표시된 이유 및 이를 수정하는 데 필요한 교정 작업에 대한 주요 정보가 포함됩니다.

사용자는 show system insecure profile 명령을 사용하여 모든 비보안 CLI 패턴의 포괄적인 목록을 볼 수도 있습니다. show system insecure configuration은 현재 적용된 제한 단계 비보안 컨피그레이션을 표시하지만, show system insecure profile은 시스템이 탐지하도록 설계된 모든 제한 단계 비보안 컨피그레이션을 표시합니다. 보안 모범 사례가 계속 발전함에 따라 프로필의 안전하지 않은 컨피그레이션 목록이 시간이 지남에 따라 업데이트됩니다.

일반적인 비보안 컨피그레이션에 대한 교정 예

이러한 예는 사용자가 일반적으로 발생하는 몇 가지 안전하지 않은 컨피그레이션을 탐지, 식별, 해결하는 방법을 보여줍니다. Cisco는 사용자가 INSECURE_CONFIG syslog 메시지를 활용하든, show system insecure 컨피그레이션 출력을 활용하든, 식별 및 차단 기능을 최대한 손쉽게 구현할 수 있도록 소프트웨어를 구현했습니다.

비보안 파일 전송 방법

디바이스에 표시되는 경고 메시지는 다음과 같습니다.

```
%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 configuration을 실행하여 이러한 비보안 컨피그레이션에 대한 추가 정보를 볼 수 있습니다.

```
<#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#
```

이러한 로그는 다음 컨피그레이션에 직접 매핑됩니다.

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

사용자는 다음 변경 사항을 통해 안전하지 않은 컨피그레이션을 완화할 수 있습니다.

<#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

안전하지 않은 레거시 SNMP 프로토콜

디바이스에 표시되는 경고 메시지입니다.

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

show system insecure configuration을 실행하여 비보안 컨피그레이션에 대한 추가 정보를 볼 수 있습니다.

<#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#
```

이러한 로그는 이 컨피그레이션에 직접 매핑됩니다.

<#root>

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

snmp-server community

RO

고객은 인증 및 암호화(authPriv)와 함께 SNMPv3를 사용하여 이 문제를 해결할 수 있습니다.

FAQ(자주 묻는 질문)

Q: Cisco에서 이러한 변화를 추진하는 이유는 무엇입니까?

A: Cisco는 안전하지 않은 레거시 기능을 비활성화하고, 더 강력한 보호 및 모니터링을 도입하고, 보안 운영을 간소화하여 네트워크 인프라의 보안 및 복원력을 향상하기 위해 이러한 변화를 추진하고 있습니다. 이러한 노력은 진화하는 사이버 위협으로부터 고객을 보호하고, 다운타임을 줄이며, 네트워크를 양자컴퓨팅과 같은 미래의 과제에 대비하도록 도와줍니다. 전반적으로 이 이니셔티브는 현재 및 미래 기술을 위한 현대적이고 안전하며 신뢰할 수 있는 기반을 구축하는 것을 목표로 합니다

Q: 안전하지 않은 컨피그레이션의 디바이스가 해당 기능의 제한 단계에서 릴리스로 업그레이드되면 어떻게 됩니까?

A : 디바이스가 특정 기능의 Restriction(Phase 2) 릴리스로 업그레이드되면 시스템은 부팅 프로세스 중에 비보안 컨피그레이션을 감지하고 디바이스를 자동으로 비보안 모드로 전환합니다.

Q: 안전하지 않은 컨피그레이션이 있는 디바이스가 해당 기능의 제거 단계에서 릴리스로 업그레이드되면 어떻게 됩니까?

A : 디바이스를 특정 기능에 대한 제거(3단계) 릴리스로 업그레이드하면 제거된 컨피그레이션을 더 이상 사용할 수 없습니다. 사용자는 폐기된 명령을 관리하기 위한 표준 마이그레이션 절차를 준수해야 합니다.

Q: 모든 안전하지 않은 기능이 동일한 릴리스에서 제거되었습니까?

A: 안전하지 않은 기능 중 일부가 동일한 릴리스에서 제거되지는 않습니다. Cisco는 단계별 접근 방식을 고수하여 안전하지 않은 기능을 세 단계로 감퇴합니다. 먼저 비보안 기능이 구성되거나 탐지되면 경고를 발효한 다음, 기본적으로 비활성화하거나 비보안 모드의 도입을 통해 명시적인 관리자 작업을 요구하여 사용을 제한하고, 마지막으로 향후 릴리스에서 기능을 완전히 제거합니다. 일부 기능은 제한 단계를 건너뛰고 경고에서 제거로 바로 이동할 수 있습니다. 제거 시기는 기능 및 플랫폼에 따라 다르며, 경고, 제한 및 제거에 대한 릴리스 번호는 Cisco IOS XE, Cisco IOS XR, Cisco NXOS, Cisco ISE 및 Cisco ASA/FTD와 같은 운영 체제마다 다릅니다. 이러한 단계적 프로세스를 통해 중단을 최소화하고 고객이 안전한 대체 제품으로 전환할 수 있도록 합니다.

Q: 안전하지 않은 기능이 제한 또는 제거 단계로 전환되는 경우는 언제입니까?

A: 안전하지 않은 기능이 제한 또는 제거 단계로 이동하는 시간은 기능 및 운영 체제에 따라 다릅니다. 자세한 내용은 기능 중단 및 제거 세부사항 설명서를 참조하십시오.

Q: 나의 특별한 불안정한 기능에 어떤 대안이 존재하는가?

A : 고객은 다양한 비보안 기능 및 프로토콜에 대한 권장 대안을 식별하기 위해 Feature Removal and Suggested Alternatives 설명서를 참조할 수 있습니다.

Q: 현재 어떤 비보안 컨피그레이션을 적용했는지 어떻게 확인할 수 있습니까?

A: 현재 어떤 제한 단계 비보안 컨피그레이션을 적용했는지 확인하려면 Cisco IOS XE 26.1.1 이상 릴리스에서 show system insecure configuration 명령을 사용할 수 있습니다. 이 명령은 디바이스에 구성된 제한 단계 비보안 기능의 포괄적인 목록을 제공합니다. 또한 Cisco SD-WAN Manager에서 Monitor(모니터링) > Advisories(권고 사항)로 이동하고 Insecure Configurations(비보안 컨피그레이션) 탭을 선택하여 디바이스, 컨피그레이션 그룹 및 템플릿 전체에서 비보안 컨피그레이션을 보고 교정 단계에 대한 링크를 볼 수 있습니다. 이 보기는 약 30분마다 새로 고쳐져 최신 정보가 보장됩니다.

Q: 특정 소프트웨어 버전에서 가능한 모든 비보안 컨피그레이션의 목록을 보려면 어떻게 해야 합니까?

A : show system insecure profile 명령을 사용하여 시스템이 탐지하도록 설계된 모든 제한 단계 비보안 CLI 패턴의 전체 목록을 볼 수 있습니다. 현재 적용된 비보안 컨피그레이션만 보여주는 show system insecure configuration과 달리, 프로필 출력에는 제한 단계에서 알려진 비보안 컨피그레이션이 모두 포함되며 보안 모범 사례가 진화함에 따라 시간이 지남에 따라 업데이트됩니다.

Q: 안전하지 않은 컨피그레이션을 수정했습니다. show system insecure 컨피그레이션 출력에 여전히 표시되는 이유는 무엇입니까?

A: 비보안 컨피그레이션에 대한 스캔은 비보안 모드에 있는 동안에만 주기적으로 실행됩니다. 즉, 안전하지 않은 컨피그레이션을 수정한 후 30분 간격으로 다음 번 예약된 스캔이 수행될 때까지 시스템에서 즉시 변경 사항을 반영할 수 없습니다. 이러한 스케줄링은 검색을 수행하는 데 필요한 오버헤드를 최소화하면서 최신 비보안 컨피그레이션 세부사항을 정기적으로 업데이트하고 표시하도록 보장합니다. test system secure all 명령을 사용하여 즉시 다시 스캔을 수행할 수 있으므로 스캔 타이머가 만료될 때까지 기다릴 필요가 없습니다.

Q: 업그레이드하기 전에 어떤 비보안 컨피그레이션을 적용했는지 사전 대응적으로 확인하려면 어떻게 해야 합니까?

A: Cisco IOS XE 17.18.2를 업그레이드하기 전에 어떤 비보안 컨피그레이션을 적용했는지 사전 대응적으로 확인하려면 고객은 Cisco Resilient Infrastructure 페이지에서 제공되는 Cisco AI Assistant for Support 봇을 사용하여 컨피그레이션을 업로드하면 비보안 기능을 식별할 수 있습니다. 유사한 툴인 Cisco Config Resilient Infrastructure Tester도 고객에게 적합한 옵션입니다. Cisco IOS XE 17.18.2 이상부터는 고객이 이러한 툴을 계속 사용할 수 있지만, 디바이스에서 show system insecure configuration 명령을 직접 실행하여 현재 적용된 비보안 컨피그레이션을 확인할 수도 있습니다. 그러나 AI Assistant for Support 봇과 Resilient Infrastructure Tester를 사용하면 직접 CLI 명령을 넘어 AI 기반 추가 증설이 가능합니다.

추가 리소스

고객은 이 설명서를 읽고 기존의 안전하지 않은 컨피그레이션에 대한 보안 모범 사례 및 대안에 대한 이해를 보완하는 것이 좋습니다.

Cisco Resilient Infrastructure - Cisco 디바이스 전반의 향상된 보안 상태로 전환하기 위한 필수 배경을 제공합니다. 사용자는 이 페이지의 오른쪽 하단에 있는 Cisco AI Assistant for Support Bot를 활용하여 다양한 출력에서 안전하지 않은 컨피그레이션을 식별하는 워크플로를 진행할 수 있습니다

Cisco Config Resilient Infrastructure Tester - 제공된 running-config를 기반으로 비보안 컨피그레이션을 확인하는 데 사용할 수 있는 툴입니다.

Cisco IOS XE Software 강화 가이드 - Cisco IOS XE 장치를 강화하고 네트워크의 전반적인 보안을 강화하는 모범 사례를 자세히 설명합니다.

기능 제거 및 권장 대안 - 최종 제거에 계획된 안전하지 않은 기능 및 프로토콜과 권장 대안 목록을 문서화합니다.

기능 사용 중단 및 제거 세부사항 - Cisco IOS XE 소프트웨어 버전을 기반으로 특정 비보안 기능 및 프로토콜이 경고 및/또는 제한 단계로 진입한 경우 문서화합니다.

SD-WAN 모니터링 및 유지 관리 가이드 - 비보안 구성 관리 장 - Cisco Catalyst SD-WAN의 비보안 기능 구성에 대한 중앙 집중식 가시성 및 실행 가능한 교정 기능을 다루며, 관리자가 네트워크 보안을 강화하고 규정 준수를 유지하기 위해 취약점을 식별하고 수정할 수 있도록 지원합니다

복원력 있는 인프라: Cisco Catalyst SD-WAN 및 라우팅 기술 참조 - Cisco Catalyst SD-WAN 및 라우팅을 위한 보안 강화 및 복원력 플레이북. CLI 및 UI 기반 관리 모델 전반에서 안전하지 않은 컨피그레이션을 식별, 교정 및 대체하기 위한 규범적 지침을 제공하며, 운영 모델 간의 일관성을 보장하면서 안전하지 않은 컨피그레이션을 안전하고 탄력적인 대안으로 전환하여 보안을 강화하고 공격 표면을 줄이며 데이터를 보호합니다

Cisco C9000 Switching Cisco IOS XE - Resilient Infrastructure Playbook - 보안 상태를 강화하고 공격 표면을 줄이며 데이터를 보호하기 위해 안전하지 않은 컨피그레이션을 식별하고 안전하고 복원력이 뛰어난 대안으로 교체하는 데 중점을 둡니다. 이 플레이북은 Catalyst 9000 제품군의 네트워크 복원력과 운영 간소화를 향상시키면서 CLI 및 UI 운영 모델 간의 일관성을 보장하는 데 목적이 있습니다

Cisco 9800 Wireless Resilient Infrastructure - Cisco의 단계별 전략에 대해 간략하게 설명합니다. 이는 안전하지 않은 기능과 프로토콜의 사용을 차단하기 위한 것으로, 소프트웨어 업그레이드 과정에서 서비스 중단을 방지하기 위한 안전한 대안을 위한 포괄적인 마이그레이션 경로를 제공합니다. 여기에는 라인 전송, 파일 전송, 관리 프로토콜 전반에 걸쳐 영향을 받는 컨피그레이션에 대한 자세한 참조 테이블과 마이그레이션 실패로 인한 잠재적 운영 영향에 대한 지침이 포함되어 있습니다

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.