유효하지 않은 SSL 컨피그레이션으로 인해 SMA에서 WSA 업그레이드 실패

목차

문제

SMA(Security Management Appliance)에서 WSA(Web Security Appliance)를 업그레이드하려고 하면 "Update failed to upgrade (Reason: 유효하지 않은 SSL 컨피그레이션)." 업그레이드는 WSA 웹 인터페이스에서 직접 수행할 경우 성공하지만, SMA에서 시작할 경우 지속적으로 실패합니다. 새 자체 서명 인증서를 생성하고 기본 인증 인증서를 변경하여 문제를 해결하려는 시도가 실패했습니다.

환경

- Cisco WSA(Web Security Appliance)
- 소프트웨어 버전: 15.2.2-009(MD)
- Cisco SMA(Security Management Appliance)
- 대상 업그레이드 버전: AsyncOS 15.5
- DNS 기능이 확인되었으며 올바르게 작동함

해결

해결 방법에는 AsyncOS 15.5의 업그레이드 전제 조건을 충족하기 위해 WSA 어플라이언스에서 레거시 TLS 버전(TLSv1.0 및 TLSv1.1)을 비활성화하는 것이 포함됩니다.

1단계: 근본 원인 파악

업그레이드 실패는 TLSv1.0 및 TLSv1.1이 프록시 컨피그레이션 이외의 SSL 컨피그레이션에서 더 이상 지원되지 않는 AsyncOS 15.5 동작의 변경으로 인해 발생합니다. 업그레이드 프로세스에서는 비 프록시 SSL 컨피그레이션에 TLSv1.2 이상이 필요합니다.

2단계: 레거시 TLS 버전 비활성화

컨피그레이션 인터페이스를 통해 WSA 어플라이언스에서 TLSv1.0 및 TLSv1.1을 비활성화합니다. 이러한 변경은 업그레이드 사전 요구 사항을 충족하며 업그레이드 프로세스를 계속 진행할 수 있도록 합니다.

3단계: 외부 서비스 호환성 확인

LDAP와 같은 외부 서비스가 TLSv1.2 이상 버전을 지원하는지 확인합니다. 이러한 서비스가 TLSv1.2 이상과 호환된다면 외부 시스템과의 통신이 중단되지 않습니다.

4단계: 업그레이드 진행

레거시 TLS 버전을 비활성화한 후 SMA에서 업그레이드 프로세스를 다시 시도하십시오. 이제 "Invalid SSL configuration(유효하지 않은 SSL 컨피그레이션)" 오류 없이 업그레이드를 진행할 수 있습니다.

5단계: 모니터링 및 검증

업그레이드 프로세스를 모니터링하여 성공적으로 완료되었는지 확인하고 모든 종속 서비스가 업그레이드 후에도 TLSv1.2에서 계속 제대로 작동하는지 확인합니다.

원인

업그레이드 실패는 AsyncOS 15.5.0-566에 도입된 동작 변경으로 인해 발생합니다. 여기서 TLSv1.0 및 TLSv1.1은 프록시 컨피그레이션 이외의 SSL 컨피그레이션에서 더 이상 지원되지 않습

니다. 이렇게 하면 AsyncOS를 업그레이드하기 전에 TLS 버전을 TLSv1.2 이상으로 변경해야 하는 업그레이드 사전 요구 사항이 생성됩니다. SMA 업그레이드 프로세스에서는 업그레이드 전 검증 검사를 수행하여 이러한 비호환성을 감지하고 업그레이드가 진행되지 않도록 방지합니다.

관련 콘텐츠

- AsyncOS 15.5 릴리스 정보
- Cisco 기술 지원 및 다운로드

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.