SX350X 또는 SX550X 스위치에서 보안 부팅

목표

이 문서의 목적은 신뢰할 수 있는 소프트웨어로만 부팅하는 방법인 보안 부팅의 프로세스를 설명하는 것입니다.이 기능은 펌웨어 버전 2.4.0.91부터 활성화됩니다.

아래 사용된 용어에 익숙하지 않은 경우 Cisco Business를 확인하십시오.새 용어 용어집.

적용 가능한 디바이스

SX350X

SX550X

소프트웨어 버전

2.4.0.91

소개

보안 부팅은 신뢰 체인을 사용하여 보안 이미지를 로드하고 실행하여 신뢰할 수 없는 소프트웨어를 로드하지 않도록 하는 방법입니다.프라이빗 키로 이미지를 할당하고 하드웨어 및 소프트웨어 메커니즘을 사용하여 로드된 이미지를 검증함으로써 신뢰 체인이 설정됩니다.이를 통해 사용자는 장치 펌웨어를 로드할 때 다른 사용자가 보안 위반 코드를 추가하지 않았는지 확인할 수 있습니다.

사용자가 새 이미지를 로드하려고 하면 새 이미지가 임시 파일로 다운로드되며, 이는 검증됩니다.오류가 발생하면 임시 파일이 삭제됩니다.이렇게 하면 새 이미지가 유효하지 않으면 설치 프로세스가 실패하고 경고 메시지가 표시됩니다.

스위치가 스태킹된 토폴로지에 있는 경우

활성(기본) 스위치에 2.4.0.91 또는 사용 가능한 최신 버전을 로드하면 스택의 모든 멤버에 펌웨어가 로드됩니다.이는 모든 디바이스에서 동일한 펌웨어를 실행해야 하기 때문에 제품군 내의 모델에 관계없이 가능합니다.스택이 정상적으로 작동합니다.

보안 부팅 프로세스

부팅 중에 시스템은 터미널에서 보안 부팅 정보를 인쇄합니다.다음은 보안 부팅 전에 디바이스에서 확인하는 단계입니다.

부팅 읽기 전용 메모리(BootROM)가 부팅 확인 상자

*부트*에서 범용 부팅(*Uboot) 확인*

*Uboot*는 *ROS 이미지 검증*

Secure Boot(보안 부팅)에서 실패를 탐지하면 디바이스가 부팅되지 않습니다.이러한 상황이 발생하면 Cisco 파트너 또는 TAC(Technical Assistance Center)에 연락하여 이 상황에서 다음 단계를 결정합니다.Cisco 파트너를 찾으려면 여기를 클릭하십시오.

보안 부팅 Syslog

부팅 중에 시스템은 보안 부팅 정보를 인쇄합니다.

보안 부팅 활성화/비활성화 - MSYS(Minimal SYStem) CPU(Central Processing Unit)와 같은 SoC(System-on-Chip) 전기 프로그래밍 가능 퓨즈(eFuse)가 없는 장치나 eFuse 보안 비트가 설정되지 않은 경우 인쇄물은 "Secure Boot disabled"가 됩니다.보안 부팅이 활성화된 경우 인쇄물은 "보안 부팅 활성화"됩니다.

BootROM*이 버튼*을 검증한 후 검증 상태(*통과/실패*)를 인쇄합니다.

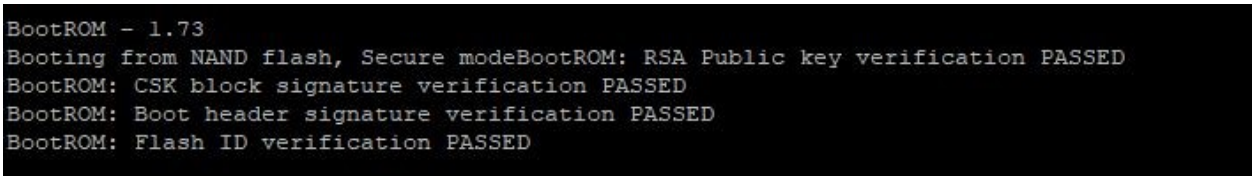
부팅 *확인* 후 검증 상태(통과/실패)가 인쇄됩니다.

Uboot*가 Ros 이미지*를 검증한 후 검증 상태(*통과/실패*)가 인쇄됩니다.

참고:오류가 발생할 경우 부팅 프로세스가 중지됩니다.

Secure Boot 출력 예 펌웨어 버전 2.4.0.91:

Secure Boot 출력 예 펌웨어 버전 2.5.0.83:



결론

이제 보안 부팅 및 보안 부팅이 네트워크를 보호하는 방법에 대해 잘 알고 있습니다.