Telepresence SUDI 인증서 체인 보안 검사 결과 트러블슈팅

목차

문제

보안 취약성 스캔은 Cisco Telepresence 비디오 코덱 엔드포인트의 SSL/TLS 인증서 관련 검색 결과, 특히 TCP 포트 4053, 4060, 4062에서 신뢰할 수 없는 인증서 체인을 보고하고 있습니다. 취약성 스캐너는 코덱을 식별하고 ACT2 SUDI CA(조직: Cisco) 인증서 체인이 Cisco Root CA 2048에서 종료되는 경우 보안 검사 시스템은 이를 조직의 보안 요구 사항을 충족하지 않는 신뢰할 수 없는 인증서 체인으로 보고합니다.

보안 스캔을 통해 보고된 구체적인 결과는 다음과 같습니다.

- 자체 서명 인증서 탐지
- 신뢰할 수 없는 인증서 체인
- 해싱 알고리즘의 취약성 문제
- 인증서 만료 경고

환경

- Cisco Telepresence 비디오 코덱 엔드포인트
- 온프레미스 등록이 가능한 Webex Desk Series 장치
- ACT2 SUDI(Secure Unique Device Identifier) 칩이 포함된 엔드포인트
- 보안 취약성 스캐닝 인프라 플래그 지정 인증서 체인 문제
- SUDI 인증서를 제공하는 TCP 포트 4053, 4060 및 4062

해결

Cisco Telepresence 엔드포인트의 SUDI 인증서는 내장된 변경 불가 인증서로서 지원되는 방식으로 수정, 재생성 또는 삭제할 수 없습니다. 이러한 인증서는 Cisco의 Trustworthy Technologies 구현 과정에 포함되며 특정 보안 기능을 제공합니다.

SUDI 인증서 동작 이해

인증서 동작은 포트 및 시스템 컨피그레이션에 따라 다릅니다.

- 포트 4053(페어링 서비스): 시스템에 ACT2 칩이 있는 경우 SUDI 인증서를 사용합니다. 사용자 지정 인증서는 ACT2 칩이 없는 시스템(이전 엔드포인트)에서만 사용됩니다.
- 포트 4047: 터치 패널과 코덱 간의 통신에 고객이 선택한 인증서를 사용합니다.

인증서 위치 및 세부 정보

SUDI 인증서는 디바이스의 인증서 저장소에 있습니다.

```
device:~] $ cd /etc/cacerts_sudi
device:/etc/cacerts_sudi] $ ls
0763c37d.0                9426d327.0                mic-cbasrcarsa4k2099.pem
29cf4e89.0                a094437b.0                mic-cmca.pem
36087b08.0                b35c8d6c.0                mic-cmca2.pem
417aa245.0                cmca2.pem                 mic-cmca3.pem
771a09b9.0                crca2048.pem              mic-cmca4.pem
89087fe6.0                crca2099.pem              mic-crcam2.pem
90359431.0                mic-cbarc2099.pem         mic-harsa-ca.pem
```

ACT2 SUDI CA 인증서 세부사항:

```
CN = ACT2 SUDI CA
O = Cisco
Valid From: Thursday, June 30, 2011 11:26:57 PM
Valid To: Tuesday, May 15, 2029 1:55:42 AM
```

권장 작업

1단계: SUDI 인증서 용도 및 보안 구현 검토

SUDI 인증서는 자체 서명되지 않았지만 Cisco Manufacturing CA에서 서명됩니다. 다음과 같은 불변의 ID 자격 증명 역할을 합니다.

- 제품 식별자 및 일련 번호 유지
- 구성, 보안, 감사 및 관리를 위해 변경할 수 없는 ID 제공
- Trust Anchor 모듈 칩에 암호로 바인딩됨
- 복제 또는 스푸핑을 사실상 불가능하게 만듭니다.

2단계: 보안 팀과 함께 SUDI 인증서 검색 결과를 제외합니다.

SUDI 인증서는 수정할 수 없으며 합법적인 보안 기능을 제공하므로 권장되는 접근 방식은 다음과 같습니다.

- 영향을 받는 서비스에 대한 SUDI 인증서 체인 검색 결과를 제외하도록 보안 검사 도구를 구성합니다
- Cisco의 Trustworthy Technologies 구현을 기반으로 예외 사항에 대한 비즈니스 사유를 문서화합니다.
- 필요한 경우 고객이 구성할 수 있는 다른 포트의 인증서에 보안 검사를 집중

3단계: 소프트웨어 업그레이드를 통한 인증서 업데이트

시스템을 최신 소프트웨어 버전으로 업그레이드할 때 신뢰 저장소에서 인증서 업데이트가 자동으로 이루어집니다. 이렇게 하면 시간이 지나도 인증서 유효성이 유지됩니다.

중요한 제한 사항

이러한 제한은 SUDI 인증서에 적용됩니다.

- 수정, 재생성 또는 삭제할 수 없음

- 인증서가 삭제되고 디바이스가 다시 시작되면 자동 재생성이 이루어집니다
- 구성 가능한 인증서를 이러한 백엔드 서비스에 할당하는 데 지원되는 방법이 없습니다.
- Trust Anchor 구현의 변경할 수 없는 특성으로 인해 인증서를 교체할 수 없습니다.

원인

보안 검사 결과는 Cisco의 SUDI(Secure Unique Device Identifier) 인증서가 있을 때 트리거됩니다. SUDI는 Cisco Root CA 2048에 연결되는 내장형 제조 인증서입니다. 이러한 인증서는 Cisco의 Trustworthy Technologies 구현 과정의 일부이며 보안 목적으로 변경할 수 없도록 설계되었습니다. 인증서는 조직별 CA가 아닌 Cisco의 루트 인증 기관에서 종료되므로 조직별 보안 검사 툴에서 신뢰하는 것으로 인식되지 않습니다. 이는 SUDI 지원 디바이스의 예상 동작이며 보안 취약성이 아닌 설계 기능을 나타냅니다.

관련 콘텐츠

- Cisco Trustworthy Technologies 데이터시트
- 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.