

인증서 기반 인증 중에 엔드포인트를 삭제하는 ISE RCM 기능

목차

문제

JAMF에서 macOS 디바이스용 Intune MDM으로 마이그레이션하는 동안 Cisco ISE는 EAP-TLS 인증 중에 엔드포인트 레코드를 예기치 않게 삭제 또는 병합하고 엔드포인트 ID 그룹 할당을 변경합니다.

영향을 받는 엔드포인트는 DB_Authorized_Devices ID 그룹에서 "엔드포인트 삭제"를 이유로 CoA 이벤트를 트리거하는 프로파일링된 엔드포인트로 이동합니다. 이로 인해 엔드포인트가 ISE 내부 데이터베이스에서 제거되고 영향을 받는 디바이스의 인증이 중단됩니다. 이 문제는 ISE가 RCM(Random and Changing MAC) 기능의 GUID로 해석하는 SAN(Subject Alternative Name) URI 필드가 포함된 동일한 인증서를 사용하여 디바이스가 무선 및 유선 연결 간에 전환할 때 발생합니다.

환경

- Cisco ISE(Identity Services Engine) 버전 3.2
- eap-TLS 인증을 사용하는 macOS 엔드포인트
- 디바이스 식별자를 포함하는 SAN URI 필드를 사용하는 인증서 기반 인증
- 무선 및 유선 네트워크 연결 간 장치 스위칭
- JAMF에서 Microsoft Intune으로의 MDM 마이그레이션
- ISE 3.2에서 기본적으로 활성화된 RCM(Random and Changing MAC) 기능
- 사용자 지정 특성이 있는 REST API를 통해 관리되는 엔드포인트

해결

이 문제는 인증서 SAN URI 필드를 기반으로 엔드포인트 레코드를 병합하는 ISE 3.2의 RCM 기능으로 인해 발생합니다. 두 가지 해결 옵션을 사용할 수 있습니다.

옵션 1: RCM 기능 비활성화(주의하여 권장)

1단계: ISE Swagger API 인터페이스 액세스

Administration(관리) > Settings(설정) > API Settings(API 설정)로 이동하고 /swagger-ui 링크를 클릭합니다.

2단계: 현재 LSD 설정 확인

Swagger 인터페이스에서 LSD Settings(LSD 설정)를 찾고 GET 요청을 실행하여 현재 컨피그레이션을 봅니다.

```
GET /api/v1/lsd/settings
```

3단계: RCM 설정 수정

RCM을 비활성화하려면 이 요청 본문으로 PUT 요청을 실행합니다.

```
{
  "enableEPO": true,
  "enableRCM": false
}
```

4단계: 컨피그레이션 변경 확인

GET 요청을 다시 실행하여 RCM이 비활성화되고 LSD가 활성화된 상태를 유지하는지 확인합니다.

5단계: 정리 스크립트 실행

RCM을 비활성화한 후 권장 스크립트 작업을 실행하여 특성 불일치를 수정합니다. 이 프로세스 중에 인프라를 모니터링하여 코너 케이스가 있는지 확인합니다.



주의: 가능해요 여기에 언급된 세부사항에는 실행될 경우 중대한 영향을 미칠 수 있는 절차 또는 명령이 포함되어 있는 것으로 보입니다. 실행 또는 권장 전에 SME 또는 사업부에서 절차 또는 명령을 평가했는지 확인하십시오.

옵션 2: 권한 부여 정책 수정

유선 및 무선 인증 흐름에 대해 별도의 권한 부여 논리를 생성하여 RCM 동작을 고려하도록 정책 집합을 조정하여 병합된 엔드포인트가 ID 그룹 멤버십만 사용하는 것이 아니라 연결 유형에 따라 적절한 액세스 결정을 받을 수 있도록 합니다.

인증서 SAN URI 처리

ISE는 특정 논리를 사용하여 인증서 SAN URI 필드를 처리하여 GUID를 추출합니다. Microsoft Entra ID 세그먼트가 포함된 인증서의 경우 ISE는 regex 패턴을 사용하여 임시 ID 세그먼트를 제거합니다.

```
tag:[a-zA-Z0-9.,-]+:sid:S-[0-9-]+[:,:]?
```

SAN URI 처리의 예:

- 입력: "ID:Meraki:GUID:673288144292101809:tag:microsoft.com,2022-09-14:sid:S-1-5-21-2942795583-2590601415-1333022741-66482"
- 세션에 저장됨: "ID:Meraki:GUID:673288144292101809"

원인

ISE 3.2에서 기본적으로 활성화된 RCM(Random and Changing MAC) 기능은 인증서 SAN URI 필드를 엔드포인트 식별을 위한 GUID로 해석합니다. 동일한 인증서를 사용하는 디바이스가 무선 및 유선 인터페이스를 통해 연결되는 경우 RCM은 공유 GUID를 기준으로 엔드포인트 레코드를 병합합니다. 이 병합 프로세스 중에 무선 엔드포인트의 특성이 유선 엔드포인트로 마이그레이션되고 무선 MAC 항목이 엔드포인트 데이터베이스에서 삭제됩니다. 이 동작은 CoA 또는 DHCP 프로브 전에 발생하며 REST API를 통해 원래 구성된 사용자 지정 특성 및 ID 그룹 할당이 손실됩니다. 병합 프로세스에서는 프로파일링 정책의 일부가 아닌 사용자 지정 특성을 보존하지 않으므로 엔드포인트 ID가 재설정되고 이후의 인증 실패가 발생합니다.

관련 콘텐츠

- [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.