세션 재인증 후 트리거되지 않는 ISE 에이전트 없는 상태 문제 해결

목차

문제

ISE(Identity Services Engine) 3.3의 에이전트 없는 포스처 기능은 세션 재인증 이벤트 후 트리거되지 않습니다. 초기 인증 중에 에이전트 없는 상태가 올바르게 작동하며 엔드포인트가 규정을 준수하게 됩니다. 그러나 재인증이 발생하면 엔드포인트가 Accounting Start 이벤트 대신 RADIUS Accounting Interim Update 이벤트를 수신하므로 에이전트 없는 상태 플로가 호출되지 않습니다. 그 결과, 엔드포인트는 알 수 없는 상태 정책과 일치하며 알 수 없는 상태 상태를 유지하므로 영향을 받는 디바이스의 네트워크 액세스에 영향을 미칩니다.

재인증 후 엔드포인트가 "포스처 보류" 또는 "알 수 없음" 상태로 고정된 상태에서 문제가 나타나며, 보고된 환경에서는 1,200개의 엔드포인트 중 약 800개가 영향을 받습니다. 로그 분석에서는 재인증 중에 ISE가 agentlessEnabled=true인 ACCOUNTING_UPDATE 이벤트를 수신하지만 포스처 플로우는 기존 세션 ID에 대해 다시 호출되지 않음을 보여줍니다.

환경

- ISE(Identity Services Engine) 버전 3.3 패치 4
- MAB(MAC Authentication Bypass)를 사용하는 유선 802.1X 인증
- 에이전트 없는 상태 컨피그레이션 사용
- 구성된 세션 재인증 타이머(420초 시간 초과)
- 네트워크 액세스 디바이스로서의 Cisco Catalyst 스위치
- 약 1,200개의 엔드포인트

해결

이 동작은 ISE의 설계에 따라 필요합니다. 에이전트 없는 상태는 RADIUS 계정 관리 시작 이벤트에

의해서만 트리거되며 프레임 IP 주소가 변경되지 않은 상태로 유지되는 경우 세션 재인증 중에 계정 관리 중간 업데이트 이벤트에 의해 다시 호출되지 않습니다.

기술 분석

ISE NetAccessEventHandler 코드 경로는 새로운 RADIUS Accounting-Start 패킷에서 에이전트 없는 포스처 흐름만 다시 암페어링합니다. 재인증 중에 네트워크 디바이스는 일반적으로 동일한 Acct-Session-Id로 Accounting Interim-Update 패킷을 보냅니다. 그러면 shouldInvokePostureFlow() 함수가 false를 반환하여 포스처 재평가를 방지합니다.

동작을 보여주는 로그 증거:

초기 인증(Agentless Posture Triggered):

```
2026-04-01 11:28:20,466 DEBUG [PrRTEvents-Executor-2][[]] cisco.cpm.posture.events.NetAccessEventHandle

2026-04-01 11:28:20,466 DEBUG [PrRTEvents-Executor-2][[]] cisco.cpm.posture.events.NetAccessEventHandle
```

재인증(에이전트 없는 상태는 트리거되지 않음):

```
2026-04-01 11:35:37,669 DEBUG [PrRTEvents-Executor-2][[]] cisco.cpm.posture.events.NetAccessEventHandle
```

권장 해결 방법

이 동작의 영향을 완화하려면 재인증 시나리오에서 엔드포인트 규정 준수를 유지하기 위해 포스처 임대 설정을 구성합니다.

1단계: 엔드포인트가 포스처 평가 간에 네트워크 액세스를 잃지 않도록 ISE 포스처 정책에서 적절한 포스처 임대 기간을 구성합니다.

2단계: 엔드포인트 포스처 상태를 모니터링하고 조직의 보안 요구 사항 및 재인증 빈도에 따라 리스 타이머를 조정합니다.

원인

이는 Cisco 버그 ID CSCwu48086에 문서화된 예상 동작입니다. ISE의 에이전트 없는 상태는 RADIUS 계정 관리 시작 이벤트에서만 트리거되도록 설계되었으며 중간 계정 관리 업데이트 이벤트에 의해 트리거되지 않습니다. 세션 재인증 중에 네트워크 액세스 디바이스는 동일한 Framed IP 주소 및 세션 ID를 사용하여 Accounting Interim Updates를 전송하며, 이는 에이전트 없는 상태 평가 프로세스를 다시 호출하지 않습니다. ISE 코드는 특별히 에이전트 없는 상태 흐름을 시작하기 전에 새 세션(ACCOUNTING_START 이벤트)을 확인합니다.

관련 콘텐츠

- Cisco 버그 ID CSCwu48086
- 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.