

링크-로컬 AAA 서버 주소를 사용하는 보안 액세스 RA VPN 인증 이벤트

목차

문제

RA(Secure Access Remote Access) VPN 기능을 테스트할 때 테넌트 조직에 없는 ID에 대해 과도한 인증 이벤트가 기록되고 있습니다. 인증 로그는 "AAALOG_SERVICE_DOWN" 및 "AAALOG_SERVER_DOWN"과 같은 AAA 오류가 포함된 24시간 동안의 10,000개 이상의 RA VPN 인증 이벤트를 표시합니다. 이러한 오류 메시지는 링크-로컬 169.254.x.x 주소를 AAA 서버로 참조하며, 이는 테넌트에 구성되지 않습니다.

로그에서 관찰되는 특정 오류 예는 다음과 같습니다.

```
AAALOG_SERVICE_DOWN
AAA authentication server not accessible : server = 169.254.169.79 : user = <user>

AAALOG_SERVER_DOWN
AAA Marking RADIUS server 169.254.169.79 as FAILED
```

이 활동은 Secure Access VPN FQDN에 대한 RADIUS 기반 인증 시도가 반복되어 과도한 로그 노이즈를 만들고 외부 스캔 또는 VPN 서비스의 잠재적인 남용에 대한 우려를 낳는 것으로 보입니다.

환경

- Cisco Secure Access 플랫폼
- 초기에 인증서 인증 없이 구성된 원격 액세스 VPN 프로파일
- RA VPN에 대해 구성된 RADIUS 기반 인증
- 검색 가능한 VPN 프로필을 사용하는 공용 VPN 테넌트 구성

해결

해결 방법에는 인증 흐름 동작을 이해하고 완화 전략으로 인증서 기반 인증을 구현하는 것이 포함되었습니다.

관찰된 행동에 대한 기술 설명

과도한 인증 이벤트는 다음 섹션에서 설명하는 기술적 이유로 인해 발생합니다.

인증서 요구 사항이 없는 인증 흐름

인증서 인증이 비활성화되고 RADIUS 기반 RA VPN 인증이 사용되는 경우, 시스템은 먼저 Secure Access에서 동기화된 사용자 데이터베이스에 대해 사용자 이름 ID를 확인하고 "실패한 권한 부여" 이벤트를 기록하므로 "실패한 권한 부여" 시도를 기록합니다. 이러한 이벤트는 1차 방어선으로 예상되지만 외부 사용자가 인증을 시도할 때 상당한 로그 노이즈를 발생시킬 수 있습니다.

링크-로컬 주소 사용

로그에 표시된 169.254.x.x 주소는 RA VPN 헤드엔드에서 수신 세션을 인증하기 위해 사용하는 내부/로컬 링크 주소입니다. 이러한 주소는 테넌트에서 AAA 서버의 잘못된 컨피그레이션이 아니라 내부 시스템 동작을 나타냅니다.

VPN 프로필 검색

공용 VPN 테넌트 ID가 구성되면 VPN 프로필이 UI 드롭다운에 나열됩니다. 이 UI에서는 외부 사용자가 공용 프로필을 더 쉽게 검색하고 인증 시도 대상으로 지정할 수 있습니다.

즉각적인 완화 단계

1.- 인증서 기반 인증을 구성합니다. 인증서 기반 인증을 요구하도록 RA VPN 프로필을 수정합니다. 인증서 인증이 필요한 경우 Secure Access는 인증 흐름에서 인증서 확인을 수행합니다. 인증서가 누락되면 표준 인증 흐름보다 먼저 오류가 발생하고 "권한 부여 실패" 이벤트가 동일한 방식으로 로깅되지 않습니다.

2.- 차단 효과 검증 인증서 기반 인증을 구현한 후 인증 로그를 모니터링하여 과도한 인증 이벤트의 감소를 확인합니다. 인증서 기반 인증으로 전환하면 공격이 성공적으로 완화되고 로그 노이즈가 감소합니다.

장기적인 개선 사항

기본 문제를 해결하기 위해 두 가지 기능 요청이 생성되었습니다.

- 기능 요청 1: 공용 VPN 테넌트가 추가될 때 터널 그룹(VPN 프로필) 목록을 숨기거나 표시하는 옵션을 추가하여 프로필 검색 가능성을 줄입니다.
- 기능 요청 2: 실패한 RA VPN 권한 부여 시도의 로깅을 활성화 또는 비활성화하는 구성 옵션을 추가하여 관리자가 로그 세부사항을 제어할 수 있도록 합니다.

또한 관리자가 정상적인 시스템 작업을 쉽게 이해할 수 있도록 로깅된 이벤트 및 인증 동작을 설명하는 공용 페이싱 문서가 생성됩니다.

원인

과도한 인증 이벤트의 근본 원인은 퍼블릭 테넌트 컨피그레이션에서 검색 가능한 VPN 프로파일과 인증서 기반 인증이 필요하지 않은 경우의 인증 흐름 동작의 조합입니다. 인증서 요구 사항 없이 RADIUS 기반 인증을 사용하는 경우, 시스템은 VPN 프로파일을 검색하는 외부 액터의 시도를 포함하여 모든 "권한 부여 실패" 시도를 보안 상태의 일부로 기록합니다. 로그의 링크-로컬 주소는 구성 오류가 아니라 RA VPN 헤드엔드 권한 부여 프로세스에 대한 정상적인 내부 시스템 동작을 나타냅니다.

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.