보안 클라이언트 ZTNA DNS 확인 및 macOS 절전 모드 후 연결 손실

목차

문제

macOS 엔드포인트의 Cisco SecureClient ZTNA는 시스템이 절전 또는 최대 절전 모드에서 다시 시작된 후 DNS 확인 실패 및 ZTA 연결 손실을 경험합니다. 이 문제는 ZTNA IA(Identity Access) 및 ZTNA PA(Private Access) 기능에 모두 영향을 미칩니다. 기본 IP 연결은 계속 작동하지만(8.8.8.8 및 208.67.222.222와 같은 외부 IP 주소에 대한 ICMP ping이 정상적으로 작동함) DNS 이름 확인에 완전히 실패하여 ZTNA를 통해 구성된 인터넷 리소스와 개인 리소스 모두에 액세스할 수 없습니다.

관찰된 특정 증상은 다음과 같습니다.

- DNS 조회는 nslookup 명령을 사용하여 실패합니다(8.8.8.8 및 208.67.222.222를 통한 www.cisco.com의 nslookup이 작동하지 않음).
- ZTNA IA 및 ZTNA PA 연결을 사용할 수 없게 됩니다.
- 엔드포인트 절전 모드 및 절전 모드 해제 주기 이후에도 지속적으로 문제가 발생합니다.
- 디바이스가 활성 상태일 때도 무작위로 문제가 발생할 수 있습니다.
- ZTNA 프로세스를 종료하면 즉시 재시작되지만 일반적으로 연결 문제가 지속됩니다.
- 전체 시스템 재부팅만 하면 전체 DNS 확인 및 ZTNA 연결이 복원됩니다.

환경

- 운영 체제: macOS(경우에 따라 문서화된 버전 26.3)
- Cisco 보안 클라이언트: 버전 5.1.14.x(5.1.16 이전의 영향 받는 버전)
- ZTNA 모듈: IA(Identity Access) 및 PA(Private Access) 컨피그레이션으로 활성

- 네트워크 모니터링: Sentinel One과 같은 서드파티 보안 솔루션을 포함할 수 있음
- 추가 보안 소프트웨어: Cisco Secure Endpoint를 포함할 수 있음
- DNS 서버: ICMP를 통해 액세스할 수 있는 외부 DNS 서버(8.8.8.8, 208.67.222.222)이지만 DNS 확인에 실패함
- UMB 모듈: 사용 중이 아님

해결

이 문제는 Cisco Engineering에서 제공한 소프트웨어 수정을 통해 해결되었습니다. 해결 프로세스에는 다음 섹션에 설명된 단계가 포함됩니다.

1단계: 문제 식별 및 버그 추적

Cisco Engineering은 이를 알려진 결함으로 식별하여 Cisco 버그 ID CSCwt24392에 "macOS: DNS는 ZTA SIA-all 및 NVM active와의 작동을 중지합니다."

2단계: 진단 데이터 수집

엔지니어링 분석을 지원하기 위해 이 진단 정보를 수집했습니다.

- 영향을 받는 엔드포인트의 DART(진단 및 보고 툴) 번들
- 패킷 캡처 파일(ZTNA Issue1.pcapng).
- 연결 실패를 보여주는 스크린샷.
- 문제 재생을 보여 주는 화면 녹화
- com.cisco.secureclient.zta.app.service 및 시스템 확장 프로세스 동작을 보여 주는 프로세스 상호 작용 로그

3단계: 엔지니어링 수정 개발

Cisco Engineering은 CSCwt24392에 대한 표적 수정을 개발하여 SecureClient 릴리스 버전 5.1.16에 포함시켰습니다. 이 수정은 특히 슬립/하이버네이션 사이클 후 macOS 시스템에서 ZTA SIA-all 및 NVM이 활성화될 때 발생하는 DNS 확인 실패를 해결합니다.

4단계: 소프트웨어 업데이트 설치

영향을 받는 macOS 엔드포인트에 Cisco SecureClient 버전 5.1.16 이상을 설치합니다. 이 버전에는 DNS 확인 및 ZTA 연결 문제에 대한 수정 사항이 포함되어 있습니다.

5단계: 검증 테스트

SecureClient 5.1.16을 설치한 후 다음 검증 단계를 수행합니다.

1.- macOS 엔드포인트가 절전 모드 또는 절전 모드로 들어가도록 허용합니다.

2.- 시스템을 절전 또는 최대 절전 모드에서 해제하십시오.

3.- nslookup 명령을 사용하여 DNS 확인 테스트

4.- 구성된 리소스에 대한 ZTNA IA 및 ZTNA PA 연결을 확인합니다.

5.- 시스템을 재부팅하지 않고도 인터넷 액세스와 개인 리소스 액세스가 모두 정상적으로 작동하는지 확인합니다.

이전 버전의 해결 방법

SecureClient 5.1.16으로 즉시 업그레이드할 수 없는 환경에서는 다음과 같은 임시 해결 방법을 사용할 수 있습니다.

- 각 절전/휴면 주기 후에 전체 시스템 재부팅을 수행하여 DNS 확인 및 ZTNA 연결을 복원합니다.
- 수면/절전 문제가 생산성에 큰 영향을 미치는 경우 ZTNA에서 일시적으로 등록을 취소하는 것을 고려하십시오(ZTNA 보호가 제거됨).

원인

이 문제의 근본 원인은 5.1.16 이전 버전의 Cisco SecureClient 소프트웨어 결함이며, 구체적으로 Cisco 버그 ID CSCwt24392으로 추적됩니다. 이 결함은 ZTA(Zero Trust Access) SIA-all(Secure Internet Access) 및 NVM(Network Visibility Module) 구성 요소가 macOS 시스템에서 활성 상태일 때 발생합니다. 절전 또는 절전 모드 및 절전 모드 해제 주기 동안 이러한 구성 요소는 기본 IP 연결을 유지하면서 DNS 확인 기능을 제대로 복원하지 못합니다. 이렇게 하면 ICMP 트래픽(ping)이 정상적으로 작동하지만 DNS 쿼리가 실패하는 상태가 만들어져 인터넷 리소스 및 ZTNA로 보호된 개인 리소스에 대한 액세스를 효과적으로 차단합니다. 이 문제는 시스템 상태 전환 중에 com.cisco.secureclient.zta.app.service 프로세스와 시스템 확장 프로세스 간의 부적절한 상호 작용과 관련이 있습니다.

관련 콘텐츠

- Cisco 버그 ID CSCwt24392 - macOS: DNS가 ZTA SIA-all 및 NVM active와의 작동을 중지합니다.
- 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.