

Secure Access XDR 통합에서 모듈 실패 오류 코드의 상태 검사 문제 해결

목차

문제

XDR과의 Cisco Secure Access 통합이 실패하고 상태 검사 단계에서 HTTP 431 "요청 헤더 필드가 너무 큼" 오류가 발생합니다. 통합은 이전에 성공적으로 수행되었지만 Cisco Secure Access 대시보드에서 생성된 API 키를 사용하여 연결을 설정하려고 할 때 갑자기 이 오류로 인해 실패하기 시작했습니다.

특정 오류 메시지는 다음과 같습니다.

<#root>

Health check of Module failed: - [v2 Reporting API] There was a client error in the Cisco Secure Access

이 오류로 인해 Secure Access 데이터가 XDR에 수집되지 않으므로 보안 가시성 및 모니터링 기능에 영향을 줍니다.

환경

- Cisco Secure Access with Advantage 라이선스
- Cisco XDR 서브스크립션
- Cisco Secure Access 테넌트
- Cisco Secure Access 대시보드 생성 키를 사용한 API 통합
- 필수 API 범위: Investigate > 읽기 전용, Reports > 읽기 전용, Deployments > 읽기 전용, Policies > 읽기/쓰기

해결

Cisco Secure Access에서 API 키와 암호를 다시 생성하여 문제가 해결되었습니다.

431 오류를 해결하려면 다음 단계를 수행하십시오.

1단계: 새 API 키 생성

Cisco Secure Access 대시보드로 이동하고 필요한 범위의 새 API 키를 만듭니다.

- 조사: 읽기 전용
- 보고서: 읽기 전용
- 구축: 읽기 전용
- 정책: 읽기/쓰기

2단계: XDR 통합에 새 키 적용

XDR Secure Access 통합 구성의 기존 API 키를 새로 생성된 키로 교체합니다.

3단계: 통합 확인

통합을 테스트하여 성공적으로 연결되었는지 확인합니다. 이제 API 호출은 431 오류가 아니라 HTTP 200 응답을 반환해야 합니다.

사전 대응적 탐지 및 방지

향후 유사한 431 오류를 식별하고 방지하려면

1.- Postman 또는 브라우저 콘솔과 같은 도구를 통해 디버깅하는 경우 요청 헤더의 크기 열을 확인합니다. 요청 헤더가 8KB(8192바이트)에 근접하거나 이를 초과하면 API 게이트웨이에서 431 오류가 발생합니다. jwt.io와 같은 외부 툴을 사용하여 OAuth 토큰 크기를 확인할 수 있습니다.

2.- 오류 패턴 분석:

- 상태 검사의 초기 핸드셰이크 중에 431 오류가 즉시 발생하는 경우 고정 자격 증명이 문제임을 나타냅니다
- 통합이 몇 분 동안 실행된 후에만 431 오류가 발생하는 경우 후속 재시도에 대한 쿠키 누적을 가리킵니다

모범 사례

헤더 크기 누적을 방지하려면 통합 클라이언트/브라우저에서 쿠키 또는 세션 지속성을 비활성화합니다.

원인

HTTP 431 오류는 표준 HTTP 권한 부여 헤더에 대해 Base64를 인코딩할 때 비정상적으로 크거나 형식이 잘못된 권한 부여 헤더를 생성하는 특정 API 키 및 비밀번호 쌍에 의해 발생했습니다.

초기 API 키의 암호화 문자열에는 일련의 문자가 포함되어 있었습니다. 이는 인코딩될 때 API 게이트웨이 제한을 초과하는 헤더 크기로 확장되어 "Request Header Fields Too Large(너무 큰 헤더 필드 요청)" 거부가 발생합니다.

API 키를 다시 생성하면 새 암호화 문자열에 적절한 크기의 권한 부여 헤더가 생성됩니다. 새 키를 해지하고 생성하는 프로세스에서는 통합 관리자측의 캐시된 요청 컨텍스트도 지워 헤더 크기를 정규화했습니다.

관련 콘텐츠

- [Cisco Secure Access API 인증](#)

- [XDR에 Cisco Secure Access 통합](#)
- [XDR 콘솔에서 HAR 로그 수집](#)
- [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.