포트 8443의 Expressway-E HTTP 보안 헤더 - 예상 동작 및 보안 스캐너 오탐

목차

문제

보안 취약성 스캐너는 TCP 포트 8443에서 Cisco Expressway-E를 검사할 때 누락된 HTTP 보안 헤더를 보고합니다. 보안 평가에서는 이러한 HTTP 보안 헤더가 누락되었고 교정을 위해 플래그가 지정되었음을 나타냅니다.

- 콘텐츠 보안 정책
- 교차 출처 포함 정책
- Cross-Origin-Opener-Policy
- 교차 출처-자원-정책
- 권한-정책
- 참조 정책
- 엄격한 전송 보안
- X-Content-Type-옵션
- X-프레임 옵션
- X-XSS 보호

조직은 이러한 헤더를 Cisco Expressway-E에서 수동으로 구성할 수 있는지, 또는 이것이 예상되는 제품 동작, 제한 사항 또는 보안 규정 준수를 위해 교정이 필요한 알려진 결함을 나타내는지 파악해야 합니다.

환경

- Cisco Expressway-E
- 포트 스캐너(예: 모바일 및 원격 액세스 환경)에서 스캔한 TCP 포트 8443을 엽니다.

해결

TCP 포트 8443에서 보고된 누락된 HTTP 보안 헤더는 예상되는 Cisco Expressway-E 동작을 나타내며 표준 웹 보안 스캐너에서 탐지될 경우 오탐으로 간주해야 합니다. 이러한 사항은 예상되는 동작을 명확히 하고 보안 규정 준수를 위한 지침을 제공합니다.

예상 동작 확인

Cisco Expressway-E의 TCP 포트 8443은 일반 브라우저 액세스 또는 표준 웹 서비스 검사를 위한 것이 아닌 HTTPS API/서비스 엔드포인트입니다. 보안 스캐너가 이 포트로 일반 또는 유효하지 않은 요청을 보낼 때 모든 HTTP 보안 헤더를 포함하지 않는 응답을 수신할 수 있습니다. 이러한 동작은 설계에 따라 필요합니다.

유효한 HTTPS 응답의 보안 헤더

Cisco Expressway-E는 유효한 HTTPS API 응답 및 합법적인 서비스 상호 작용에 적절한 보안 헤더를 포함합니다. 헤더는 적절한 API 호출을 통해 포트에 올바르게 액세스할 때 또는 Webex 로그인 프로세스와 같은 유효한 인증 흐름 중에 존재합니다. Expressway에서 진단 로그를 수집하여 이를 확인합니다.

포트 8443의 유효한 HTTPS 응답에 있는 보안 헤더의 예:

```
HTTP/1.1 200
x-frame-options: SAMEORIGIN
strict-transport-security: max-age=31536000; includeSubdomains
x-content-type-options: nosniff
x-xss-protection: 1; mode=block
content-security-policy: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval';style-src
content-type: application/soap+xml;charset=UTF-8
content-length: 474
date: Thu, 12 Feb 2026 08:52:05 GMT
server:
Age: 0
Connection: keep-alive
```

포트 443의 API 응답에서 보안 헤더의 예:

```
HTTP/1.1 201 Created
Date: Mon, 22 Jul 2024 21:22:00 GMT
Server: VCS
Referrer-Policy: same-origin
Permissions-Policy: geolocation=();
Content-Security-Policy: default-src 'self';base-uri 'self';block-all-mixed-content;child-src 'self';co
Strict-Transport-Security: max-age=31556926; includeSubDomains
X-Frame-Options: sameorigin
X-Content-Type-Options: nosniff
X-WebKit-CSP: self
X-Permitted-Cross-Domain-Policies: none
X-XSS-Protection: 1; mode=block
Content-Type: application/json
Location: /provisioning/common/dns/dnsserver/index/2
Transfer-Encoding: chunked
Content-Language: en
```

스캐너 응답 예

적절한 API 컨텍스트 없이 일반 스캐너 또는 컬 요청이 포트 8443에 제출되면 제한된 헤더가 포함된 400개의 잘못된 요청 응답을 수신합니다. TCP 포트 8443은 API 요청을 통하지 않는 한 (예: 브라우저에서) 액세스해서는 안 됩니다.

```
HTTP/1.1 400 Bad Request
Date: Fri, 26 Jun 2026 21:35:58 GMT
Connection: close
Strict-Transport-Security: max-age=31536000; includeSubDomains
Server: CE_E
Cache-Control: no-store
Content-Type: text/html
Content-Language: en
Content-Length: 65
```

보안 헤더 컨피그레이션

HTTP 보안 헤더는 Cisco Expressway-E에서 사용자가 구성할 수 없습니다. 이러한 헤더는 Expressway 소프트웨어에 의해 완전히 제어되며 요청 및 서비스 상호 작용의 유형에 따라 적절한 응답에 자동으로 포함됩니다.

원인

Cisco Expressway-E의 TCP 포트 8443은 일반 HTTP 요청을 통해 액세스할 수 있는 표준 웹 서비스 포트가 아니라 특정 서비스 통신을 위한 HTTPS API 엔드포인트로 설계되었습니다. 이 포트로 일반 요청 또는 잘못된 요청을 보내는 보안 스캐너는 HTTP 보안 헤더의 전체 보수가 포함되지 않은 400개의 잘못된 요청 응답을 수신합니다. 이 동작은 Cisco Bug ID CSCvt86137에 설명되어 있습니다. 여기서 개발자는 보안 헤더의 중요성이 렌더링되는 콘텐츠에 따라 다르다고 판단했으며 Expressway는 이미 적절한 경우 보안 헤더를 사용합니다.

헤더가 합법적인 API 상호 작용 및 서비스 플로우에 존재하기 때문에 스캐너 응답에 헤더가 없다는 것은 보안 취약성이 아니라 예상된 제품 동작을 나타냅니다.

관련 콘텐츠

- Cisco Expressway IP 포트 사용 컨피그레이션 가이드 - 모바일 및 원격 액세스
- Cisco 버그 ID CSCvt86137 - Expressway의 HTTP 응답에 있는 보안 헤더
- Cisco 버그 ID CSCvx01616 - 포트 스캐너 응답의 Strict-Transport-Security 헤더
- 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.