Expressway-E HTTP Security Header auf Port 8443 - Erwartetes Verhalten und Sicherheitsscanner - Fehlalarme

Inhalt

Problem

Sicherheitsscanner melden fehlende HTTP-Sicherheits-Header beim Scannen von Cisco Expressway-E auf dem TCP-Port 8443. Die Sicherheitsbewertung zeigt an, dass diese HTTP-Sicherheits-Header fehlen und zur Behebung gekennzeichnet sind:

- Content-Security-Policy
- Cross-Origin-Embedder-Policy
- Cross-Origin-Opener-Policy
- Ursprungsübergreifende Ressourcenrichtlinie
- Berechtigungs-Policy
- Referrer-Richtlinie
- Strict-Transport-Security
- X-Inhaltstyp-Optionen
- X-Frame-Optionen
- X-XSS-Schutz

Unternehmen müssen sich darüber im Klaren sein, ob diese Header manuell auf Cisco Expressway-E konfiguriert werden können, oder ob es sich dabei um ein erwartetes Produktverhalten, eine Einschränkung oder einen bekannten Fehler handelt, der behoben werden muss, um die Einhaltung der Sicherheitsvorschriften zu gewährleisten.

Umwelt

- Cisco Expressway E
- Offener, vom Port-Scanner gescannter TCP-Port 8443 (z. B. Mobile und Remote Access-Umgebung)

Auflösung

Die gemeldeten fehlenden HTTP-Sicherheits-Header am TCP-Port 8443 stellen das erwartete Cisco Expressway-E-Verhalten dar und müssen als falsch positiv eingestuft werden, wenn sie von Standard-Websicherheits-Scannern erkannt werden. Diese Punkte verdeutlichen das erwartete Verhalten und geben Hinweise für die Einhaltung von Sicherheitsrichtlinien:

Erwartete Verhaltensbestätigung

Der TCP-Port 8443 auf Cisco Expressway-E ist ein HTTPS-API/Service-Endpunkt, der nicht für den allgemeinen Browserzugriff oder standardmäßige Webservice-Scans vorgesehen ist. Wenn Sicherheitsscanner generische oder ungültige Anfragen an diesen Port senden, können sie Antworten empfangen, die nicht alle HTTP-Sicherheits-Header enthalten. Dieses Verhalten wird erwartet und ist geplant.

Sicherheitsheader in gültigen HTTPS-Antworten

Cisco Expressway-E enthält die entsprechenden Sicherheits-Header in gültigen HTTPS-API-Antworten und legitimen Service-Interaktionen. Die Header sind vorhanden, wenn über ordnungsgemäße API-Aufrufe oder während gültiger Authentifizierungsprozesse wie WebEx Anmeldeprozesse auf den Port zugegriffen wird. Überprüfen Sie dies, indem Sie Diagnoseprotokolle von Expressway sammeln.

Beispiel für Sicherheitskopfzeilen in gültiger HTTPS-Antwort auf Port 8443:

```
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
```

Beispiel für Sicherheits-Header in API-Antwort auf Port 443:

```
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
```

Beispiel für Scanner-Antwort

Wenn generische Scanner oder Curl-Anfragen ohne richtigen API-Kontext an Port 8443 gesendet werden, erhalten sie eine Antwort mit 400 ungültigen Anfragen und begrenzten Headern. Der TCP-Port 8443 ist nur über API-Anfragen für den Zugriff (z. B. über einen Browser) vorgesehen.

```
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
```

Security Header-Konfiguration

HTTP-Sicherheits-Header können auf Cisco Expressway-E nicht vom Benutzer konfiguriert werden. Diese Header werden vollständig von der Expressway-Software gesteuert und automatisch in die entsprechenden Antworten aufgenommen, je nach Art der Anfrage und der Interaktion mit dem Service.

Ursache

Der TCP-Port 8443 auf Cisco Expressway-E ist als HTTPS-API-Endpunkt für bestimmte Servicekommunikationen konzipiert, nicht als Standard-Web-Service-Port, auf den über generische HTTP-Anfragen zugegriffen werden kann. Sicherheitsscanner, die generische oder ungültige Anfragen an diesen Port senden, erhalten 400 Antworten auf fehlerhafte Anfragen, die nicht die vollständige Ergänzung der HTTP-Sicherheits-Header enthalten. Dieses Verhalten ist in Cisco Bug-ID CSCvt86137 dokumentiert, wo Entwickler festgestellt haben, dass die Bedeutung von Sicherheits-Headern vom gerenderten Inhalt abhängt, und Expressway ggf. bereits Sicherheits-Header verwendet.

Das Fehlen von Headern in Scanner-Antworten stellt eher ein erwartetes Produktverhalten als eine Sicherheitslücke dar, da die Header in legitimen API-Interaktionen und Service-Flows vorhanden sind.

Verwandte Inhalte

- Cisco Expressway IP Port Usage Configuration Guide - Mobiler und Remote-Zugriff
- Cisco Bug-ID CSCvt86137 - Sicherheits-Header in HTTP-Antworten von Expressway
- Cisco Bug-ID CSCvx01616 - Strict-Transport-Security-Header in Port-Scanner-Antworten
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.