Expressway-E HTTP-beveiligingskoppen op poort 8443 - Verwachte gedrag- en beveiligingsscanner met valse positieven

Inhoud

uitgifte

Beveiligingsbeveiligingsscanners melden ontbrekende HTTP-beveiligingshoofdstukken bij het scannen van Cisco Expressway-E op TCP-poort 8443. De beveiligingsbeoordeling geeft aan dat deze HTTP-beveiligingshoofdstukken ontbreken en gemarkeerd zijn voor herstel:

- beleid inzake inhoudbeveiliging
- cross-origin-embedder-policy
- cross-origin-opener-beleid
- beleid inzake de kruiselingse oorsprong van hulpbronnen
- machtigingsbeleid
- verwijzingsbeleid
- strikte beveiliging van het vervoer
- X-Content-Type-Opties
- X-frame-opties
- X-XSS-bescherming

Organisaties moeten begrijpen of deze headers handmatig kunnen worden geconfigureerd op Cisco Expressway-E, of dat dit het verwachte productgedrag, een beperking of een bekend defect vertegenwoordigt dat moet worden verholpen om aan de beveiligingsvereisten te voldoen.

milieu

- Cisco Expressway-E
- Open TCP-poort 8443 gescand door poortscanner (zoals mobiele en externe toegangsomgeving)

resolutie

De gemelde ontbrekende HTTP-beveiligingshoofdkoppen op TCP-poort 8443 vertegenwoordigen het verwachte Cisco Expressway-E-gedrag en moeten als vals positief worden beschouwd wanneer ze worden gedetecteerd door standaard webbeveiligingsscanners. Deze punten verduidelijken het verwachte gedrag en bieden richtlijnen voor de naleving van de beveiligingsvoorschriften:

Verwachte gedragsbevestiging

TCP-poort 8443 op Cisco Expressway-E is een HTTPS API/service-eindpunt dat niet bedoeld is voor algemene browsertoegang of standaard webservicescanning. Wanneer beveiligingsscanners generieke of ongeldige verzoeken naar deze poort verzenden, kunnen ze antwoorden ontvangen die niet alle HTTP-beveiligingshoofdkoppen bevatten. Dit gedrag wordt verwacht en door het ontwerp.

Beveiligingshoofdkoppen in geldige HTTPS-antwoorden

Cisco Expressway-E bevat de juiste beveiligingshoofdkoppen in geldige HTTPS API-antwoorden en legitieme serviceinteracties. De headers zijn aanwezig wanneer de poort correct wordt benaderd via de juiste API-aanroepen of tijdens geldige verificatiestromen zoals Webex-aanmeldingsprocessen. Controleer dit door diagnostische logboeken te verzamelen op de snelweg.

Voorbeeld van beveiligingshoofdkoppen in een geldige HTTPS-respons op poort 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
```

Voorbeeld van beveiligingshoofdkoppen in API-respons op poort 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
```

Voorbeeld scannerrespons

Wanneer generieke scanners of curl-verzoeken worden gedaan naar poort 8443 zonder de juiste API-context, ontvangen ze een 400 Bad Request-antwoord met beperkte headers. TCP-poort 8443 is niet bedoeld voor toegang (zoals door een browser), behalve via API-verzoeken.

```
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
```

Beveiligingskopconfiguratie

HTTP-beveiligingshoofdkoppen zijn niet door de gebruiker te configureren op Cisco Expressway-E. Deze headers worden volledig beheerd door de Expressway-software en worden automatisch opgenomen in de juiste antwoorden op basis van het type aanvraag en serviceinteractie.

Oorzaak

TCP-poort 8443 op Cisco Expressway-E is ontworpen als een HTTPS API-eindpunt voor specifieke servicecommunicatie, niet als een standaard webservicepoort die toegankelijk is via algemene HTTP-verzoeken. Beveiligingsscanners die generieke of ongeldige verzoeken naar deze poort verzenden, ontvangen 400 antwoorden op een onjuist verzoek die niet het volledige complement van HTTP-beveiligingshoofdkoppen bevatten. Dit gedrag is gedocumenteerd in Cisco Bug ID CSCvt86137, waar ontwikkelaars hebben vastgesteld dat het belang van beveiligingshoofdkoppen afhangt van de inhoud die wordt weergegeven, en de Expressway gebruikt waar nodig al beveiligingshoofdkoppen.

Het gebrek aan headers in scannerreacties vertegenwoordigt verwacht productgedrag in plaats van een beveiligingslek, omdat de headers aanwezig zijn in legitieme API-interacties en servicestroom.

Gerelateerde inhoud

- Configuratiegids voor gebruik van Cisco Expressway IP-poorten - Mobiele en externe toegang
- Cisco Bug ID CSCvt86137 - Beveiligingshoofdkoppen in HTTP-reacties van Expressway
- Cisco Bug ID CSCvx01616 - Strikt-Transport-Security header in reacties op poortscanners
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.