Expressway-E HTTP Security Headers on Port 8443 - Expected Behavior and Security Scanner False Positives

Contents

Issue

Security vulnerability scanners report missing HTTP security headers when scanning Cisco Expressway-E on TCP port 8443. The security assessment indicates that these HTTP security headers are missing and flagged for remediation:

- Content-Security-Policy
- Cross-Origin-Embedder-Policy
- Cross-Origin-Opener-Policy
- Cross-Origin-Resource-Policy
- Permissions-Policy
- Referrer-Policy
- Strict-Transport-Security
- X-Content-Type-Options
- X-Frame-Options
- X-XSS-Protection

Organizations need to understand whether these headers can be manually configured on Cisco Expressway-E, or if this represents expected product behavior, a limitation, or a known defect that requires remediation for security compliance purposes.

Environment

- Cisco Expressway-E

- Open TCP port 8443 scanned by port scanner (such as Mobile and Remote Access environment)

Resolution

The reported missing HTTP security headers on TCP port 8443 represent expected Cisco Expressway-E behavior and must be considered a false positive when detected by standard web security scanners. These points clarify the expected behavior and provide guidance for security compliance:

Expected Behavior Confirmation

TCP port 8443 on Cisco Expressway-E is an HTTPS API/service endpoint that is not intended for generic browser access or standard web service scanning. When security scanners send generic or invalid requests to this port, they can receive responses that do not include all HTTP security headers. This behavior is expected and by design.

Security Headers in Valid HTTPS Responses

Cisco Expressway-E does include the appropriate security headers in valid HTTPS API responses and legitimate service interactions. The headers are present when the port is accessed correctly through proper API calls or during valid authentication flows such as Webex login processes. Check this by collecting diagnostic logs from the Expressway.

Example of security headers present in valid HTTPS response on 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
```

Example of security headers in API response on 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
```

Scanner Response Example

When generic scanners or curl requests are made to port 8443 without proper API context, they receive a 400 Bad Request response with limited headers. TCP port 8443 is not intended to be accessed (such as by a browser) except via API requests.

```
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 Configuration

HTTP security headers are not user-configurable on Cisco Expressway-E. These headers are controlled entirely by the Expressway software and are included automatically in appropriate responses based on the type of request and service interaction.

Cause

TCP port 8443 on Cisco Expressway-E is designed as an HTTPS API endpoint for specific service communications, not as a standard web service port accessible through generic HTTP requests. Security scanners that send generic or invalid requests to this port receive 400 Bad Request responses that do not include the full complement of HTTP security headers. This behavior is documented in Cisco Bug ID CSCvt86137, where developers determined that the significance of security headers depends on the content being rendered, and the Expressway already uses security headers where appropriate.

The lack of headers in scanner responses represents expected product behavior rather than a security vulnerability, as the headers are present in legitimate API interactions and service flows.

Related Content

- Cisco Expressway IP Port Usage Configuration Guide - Mobile and Remote Access
- Cisco Bug ID CSCvt86137 - Security headers in HTTP responses from Expressway
- Cisco Bug ID CSCvx01616 - Strict-Transport-Security header in port scanner responses
- Cisco Technical Support & Downloads