埠8443上的Expressway-E HTTP安全報頭 — 預期行為和安全掃描程式誤報

目錄

問題

安全漏洞掃描程式在TCP埠8443上掃描Cisco Expressway-E時報告缺少HTTP安全標頭。安全評估表明這些HTTP安全標頭缺失並標籤以進行修復：

- Content-Security-Policy
- 跨源嵌入策略
- 跨來源 — Opener-Policy
- 跨源資源策略
- 許可權 — 策略
- Referrer策略
- Strict-Transport-Security
- X-Content-Type-Options
- X-Frame-Options
- X-XSS-Protection

組織需要瞭解是否可在Cisco Expressway-E上手動配置這些報頭，或者這是否代表預期的產品行為、限制或已知缺陷，需要出於安全合規目的進行補救。

環境

- Cisco Expressway-E

- 由埠掃描器（例如移動和遠端訪問環境）掃描的開放式TCP埠8443

解析

報告的TCP埠8443上缺少HTTP安全報頭表示預期的Cisco Expressway-E行為，標準網路安全掃描器檢測到此行為時，必須將其視為誤報。以下幾點可澄清預期行為，並為安全合規性提供指導：

預期行為確認

Cisco Expressway-E上的TCP埠8443是HTTPS API/服務終結點，不適用於普通瀏覽器訪問或標準Web服務掃描。當安全掃描程式向此埠傳送一般或無效請求時，它們可以接收不包括所有HTTP安全標頭的響應。這是預期行為，也是設計行為。

有效HTTPS響應中的安全標頭

Cisco Expressway-E在有效的HTTPS API響應和合法服務互動中確實包含適當的安全標頭。當連線埠透過適當的API呼叫正確存取時，或有效的驗證流程（例如Webex登入程式）期間，就會顯示標頭。通過從Expressway收集診斷日誌來檢查這一點。

埠8443上的有效HTTPS響應中存在安全標頭的示例：

```
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
```

連線埠443上API回應中的安全標頭範例：

```
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
```

掃描器響應示例

當通用掃描程式或捲曲請求被傳送到沒有適當API上下文的埠8443時，它們會收到400個包含有限標頭的Bad Request響應。除非通過API請求，否則不允許訪問TCP埠8443（例如通過瀏覽器）。

```
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
```

安全標頭配置

使用者無法在Cisco Expressway-E上配置HTTP安全標頭。這些報頭完全由Expressway軟體控制，並根據請求型別和服務互動自動包含在適當的響應中。

原因

Cisco Expressway-E上的TCP埠8443設計為用於特定服務通訊的HTTPS API終結點，而不是通過通用HTTP請求訪問的標準Web服務埠。向此埠傳送常規或無效請求的安全掃描程式收到400個不包含HTTP安全標頭完整補充的錯誤請求響應。此行為記錄在Cisco錯誤ID CSCvt86137中，開發人員確定安全標頭的意義取決於呈現的內容，並且Expressway已在適當的情況下使用安全標頭。

掃描程式響應中缺少標頭表示預期的產品行為，而不是安全漏洞，因為標頭存在於合法API互動和服務流中。

相關內容

- Cisco Expressway IP埠使用配置指南 — 移動和遠端訪問
- 思科錯誤ID CSCvt86137 — 來自Expressway的HTTP響應中的安全標頭
- 思科錯誤ID CSCvx01616 — 埠掃描程式響應中的Strict-Transport-Security標頭
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。