端口8443上的Expressway-E HTTP安全报头 — 预期行为和安全扫描程序误报

目录

问题

安全漏洞扫描程序报告在TCP端口8443上扫描Cisco Expressway-E时缺少HTTP安全报头。安全评估表明这些HTTP安全标头缺失并标记用于修复：

- 内容安全策略
- 跨源 — 嵌入者策略
- Cross-Origin-Open-Policy
- 跨源资源策略
- 权限策略
- Referrer策略
- Strict-Transport-Security
- X-Content-Type-Options
- X-Frame-Options
- X-XSS-Protection

组织需要了解是否可在Cisco Expressway-E上手动配置这些报头，或者这是否代表预期的产品行为、限制或已知缺陷，需要出于安全合规目的进行补救。

环境

- Cisco Expressway-E

- 由端口扫描程序（例如移动和远程访问环境）扫描的开放TCP端口8443

分辨率

TCP端口8443上报告的缺失HTTP安全报头代表预期的Cisco Expressway-E行为，在标准网络安全扫描仪检测到时，必须将其视为误报。以下几点可澄清预期行为，并为安全合规性提供指导：

预期行为确认

Cisco Expressway-E上的TCP端口8443是HTTPS API/服务终端，不适用于通用浏览器访问或标准Web服务扫描。当安全扫描程序向此端口发送一般或无效请求时，它们会收到不包含所有HTTP安全报头的响应。此行为是预期行为，且是设计行为。

有效HTTPS响应中的安全信头

Cisco Expressway-E在有效的HTTPS API响应和合法服务交互中包含相应的安全报头。通过适当的API调用正确访问端口或有效身份验证流程（例如Webex登录流程）期间存在报头。通过从Expressway收集诊断日志来检查这一点。

端口8443上的有效HTTPS响应中存在的安全报头示例：

```
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
```

端口443上API响应中的安全报头示例：

```
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
```

扫描仪响应示例

当通用扫描程序或卷曲请求发送到没有适当API情景的端口8443时，它们会收到400个包含有限报头的错误请求响应。除非通过API请求，否则不得访问TCP端口8443（例如通过浏览器）。

```
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
```

安全报头配置

HTTP安全标头在Cisco Expressway-E上不可由用户配置。这些报头完全由Expressway软件控制，并根据请求类型和服务交互自动包含在适当的响应中。

原因

Cisco Expressway-E上的TCP端口8443设计为用于特定服务通信的HTTPS API终端，而不是通过通用HTTP请求可访问的标准Web服务端口。向此端口发送一般或无效请求的安全扫描程序会收到400个不包含HTTP安全报头完整补充的错误请求响应。此行为记录在Cisco Bug ID CSCvt86137中，开发人员确定安全报头的意义取决于所呈现的内容，并且Expressway已在适当的情况下使用安全报头。

扫描程序响应中缺少报头表示预期的产品行为，而不是安全漏洞，因为报头存在于合法API交互和服务流中。

相关内容

- Cisco Expressway IP端口使用配置指南 — 移动和远程访问
- Cisco Bug ID CSCvt86137 — 来自Expressway的HTTP响应中的安全报头
- Cisco Bug ID CSCvx01616 — 端口扫描程序响应中的Strict-Transport-Security报头
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。