Encabezados de seguridad HTTP de Expressway-E en el puerto 8443: comportamiento esperado y falsos positivos del analizador de seguridad

Contenido

Problema

Los analizadores de vulnerabilidades de seguridad informan de la ausencia de encabezados de seguridad HTTP al analizar Cisco Expressway-E en el puerto TCP 8443. La evaluación de seguridad indica que faltan estos encabezados de seguridad HTTP y que están marcados para su corrección:

- Content-Security-Policy
- Cross-Origin-Embedded-Policy
- Cross-Origin-Opener-Policy
- Cross-Origin-Resource-Policy
- Directiva de permisos
- Política de referencia
- Seguridad de transporte estricta
- X-Content-Type-Options
- Opciones de marco X
- Protección X-XSS

Las organizaciones deben saber si estos encabezados se pueden configurar manualmente en Cisco Expressway-E o si esto representa un comportamiento esperado del producto, una limitación o un defecto conocido que requiere remediación por motivos de seguridad.

Entorno

- Cisco Expressway-E
- Abra el puerto TCP 8443 analizado por el analizador de puertos (como el entorno de acceso remoto y móvil).

Resolución

Los encabezados de seguridad HTTP faltantes notificados en el puerto TCP 8443 representan el comportamiento esperado de Cisco Expressway-E y se debe considerar un falso positivo cuando lo detectan los analizadores de seguridad web estándar. Estos puntos aclaran el comportamiento esperado y proporcionan orientación para el cumplimiento de la seguridad:

Confirmación de comportamiento esperado

El puerto TCP 8443 de Cisco Expressway-E es un extremo de servicio/API HTTPS que no está pensado para el acceso genérico al navegador ni para el análisis estándar de servicios web. Cuando los analizadores de seguridad envían solicitudes genéricas o no válidas a este puerto, pueden recibir respuestas que no incluyen todos los encabezados de seguridad HTTP. Se espera este comportamiento y por diseño.

Encabezados de seguridad en respuestas HTTPS válidas

Cisco Expressway-E incluye los encabezados de seguridad adecuados en las respuestas de API HTTPS válidas y las interacciones de servicio legítimas. Los encabezados están presentes cuando se accede correctamente al puerto a través de llamadas API adecuadas o durante flujos de autenticación válidos como procesos de inicio de sesión de Webex. Para comprobarlo, recopile los registros de diagnóstico de Expressway.

Ejemplo de encabezados de seguridad presentes en una respuesta HTTPS válida en el puerto 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
```

Ejemplo de encabezados de seguridad en la respuesta de API en el puerto 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
```

Ejemplo de respuesta del escáner

Cuando los analizadores genéricos o las solicitudes curl se realizan al puerto 8443 sin el contexto de API apropiado, reciben una respuesta 400 Bad Request con encabezados limitados. No se pretende acceder al puerto TCP 8443 (por ejemplo, a través de un navegador), excepto a través de solicitudes de API.

```
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
```

Configuración del encabezado de seguridad

Los encabezados de seguridad HTTP no son configurables por el usuario en Cisco Expressway-E. Estos encabezados son controlados totalmente por el software Expressway y se incluyen automáticamente en las respuestas apropiadas en función del tipo de solicitud e interacción del servicio.

Causa

El puerto TCP 8443 de Cisco Expressway-E está diseñado como un extremo de la API HTTPS para comunicaciones de servicio específicas, no como un puerto de servicio web estándar al que se puede acceder a través de solicitudes HTTP genéricas. Los analizadores de seguridad que envían solicitudes genéricas o no válidas a este puerto reciben 400 respuestas de solicitudes incorrectas que no incluyen el complemento completo de encabezados de seguridad HTTP. Este comportamiento se documenta en Cisco Bug ID CSCvt86137, donde los desarrolladores determinaron que la importancia de los encabezados de seguridad depende del contenido que se está representando, y Expressway ya utiliza encabezados de seguridad cuando es apropiado.

La falta de encabezados en las respuestas del analizador representa el comportamiento esperado del producto en lugar de una vulnerabilidad de seguridad, ya que los encabezados están presentes en las interacciones legítimas de API y en los flujos de servicios.

Contenido relacionado

- Guía de configuración de uso de puertos IP de Cisco Expressway - Acceso móvil y remoto
- Cisco Bug ID CSCvt86137 - Encabezados de seguridad en respuestas HTTP de Expressway
- Cisco Bug ID CSCvx01616 - Encabezado Strict-Transport-Security en las respuestas del analizador de puertos
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).