Cabeçalhos de segurança HTTP do Expressway-E na porta 8443 - comportamento esperado e falsos positivos do scanner de segurança

Contents

Problema

Os verificadores de vulnerabilidade de segurança relatam a ausência de cabeçalhos de segurança HTTP ao verificar o Cisco Expressway-E na porta TCP 8443. A avaliação de segurança indica que esses cabeçalhos de segurança HTTP estão ausentes e sinalizados para correção:

- Content-Security-Policy
- Cross-Origin-Embedder-Policy
- Política de Abertura de Origem Cruzada
- Política-recurso-origem-cruzada
- Permissões-Política
- Política de referência
- Strict-Transport-Security
- X-Content-Type-Options
- X-Frame-Options
- X-XSS-Protection

As empresas precisam entender se esses cabeçalhos podem ser configurados manualmente no Cisco Expressway-E ou se isso representa o comportamento esperado do produto, uma limitação ou um defeito conhecido que exija correção para fins de conformidade de segurança.

Ambiente

- Cisco Expressway-E
- Abra a porta TCP 8443 verificada pelo scanner de porta (como ambiente de acesso remoto e móvel)

Resolução

Os cabeçalhos de segurança HTTP ausentes relatados na porta TCP 8443 representam o comportamento esperado do Cisco Expressway-E e devem ser considerados falsos positivos quando detectados por verificadores de segurança da Web padrão. Estes pontos esclarecem o comportamento esperado e fornecem orientação para conformidade de segurança:

Confirmação de comportamento esperada

A porta TCP 8443 no Cisco Expressway-E é um ponto de extremidade de API/serviço HTTPS que não se destina ao acesso genérico do navegador ou à verificação de serviço Web padrão. Quando os verificadores de segurança enviam solicitações genéricas ou inválidas a essa porta, eles podem receber respostas que não incluem todos os cabeçalhos de segurança HTTP. Esse comportamento é esperado e planejado.

Cabeçalhos de segurança em respostas HTTPS válidas

O Cisco Expressway-E inclui os cabeçalhos de segurança apropriados em respostas de API HTTPS válidas e interações de serviço legítimas. Os cabeçalhos estão presentes quando a porta é acessada corretamente por meio de chamadas de API apropriadas ou durante fluxos de autenticação válidos, como processos de login do Webex. Verifique isso coletando logs de diagnóstico do Expressway.

Exemplo de cabeçalhos de segurança presentes em uma resposta HTTPS válida na porta 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
```

Exemplo de cabeçalhos de segurança na resposta da API na porta 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
```

Exemplo de resposta do scanner

Quando scanners genéricos ou solicitações curl são feitos para a porta 8443 sem o contexto de API apropriado, eles recebem uma resposta 400 Bad Request com cabeçalhos limitados. A porta TCP 8443 não deve ser acessada (por exemplo, por um navegador), exceto por solicitações 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
```

Configuração do cabeçalho de segurança

Os cabeçalhos de segurança HTTP não são configuráveis pelo usuário no Cisco Expressway-E. Esses cabeçalhos são totalmente controlados pelo software Expressway e são incluídos automaticamente nas respostas apropriadas com base no tipo de solicitação e interação de serviço.

Causa

A porta TCP 8443 no Cisco Expressway-E foi projetada como um ponto de extremidade de API HTTPS para comunicações de serviço específicas, não como uma porta de serviço Web padrão acessível por solicitações HTTP genéricas. Os verificadores de segurança que enviam solicitações genéricas ou inválidas para esta porta recebem 400 respostas de Solicitação Incorreta que não incluem o complemento completo de cabeçalhos de segurança HTTP. Esse comportamento é documentado na ID de bug Cisco CSCvt86137, onde os desenvolvedores determinaram que a importância dos cabeçalhos de segurança depende do conteúdo que está sendo renderizado, e o Expressway já usa cabeçalhos de segurança quando apropriado.

A falta de cabeçalhos nas respostas do scanner representa o comportamento esperado do produto, e não uma vulnerabilidade de segurança, pois os cabeçalhos estão presentes em interações de API legítimas e fluxos de serviço.

Conteúdo relacionado

- Guia de configuração de uso da porta IP do Cisco Expressway - Acesso móvel e remoto
- ID de bug Cisco CSCvt86137 - Cabeçalhos de segurança em respostas HTTP do Expressway
- ID de bug Cisco CSCvx01616 - cabeçalho Strict-Transport-Security nas respostas do scanner de porta
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.