En-têtes de sécurité HTTP Expressway-E sur le port 8443 - Comportement attendu et faux positifs du scanneur de sécurité

Table des matières

Problème

Les analyseurs de vulnérabilité signalent des en-têtes de sécurité HTTP manquants lors de l’analyse de Cisco Expressway-E sur le port TCP 8443. L'évaluation de la sécurité indique que ces en-têtes de sécurité HTTP sont manquants et marqués pour correction :

- 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
- Protection X-XSS

Les entreprises doivent déterminer si ces en-têtes peuvent être configurés manuellement sur Cisco Expressway-E ou s’il s’agit d’un comportement attendu du produit, d’une limitation ou d’un défaut connu qui nécessite une correction à des fins de conformité de la sécurité.

Environnement

- Cisco Expressway-E
- Ouvrir le port TCP 8443 analysé par l'analyseur de port (tel que l'environnement d'accès mobile et distant)

Résolution

Les en-têtes de sécurité HTTP manquants signalés sur le port TCP 8443 représentent le comportement attendu de Cisco Expressway-E et doivent être considérés comme des faux positifs lorsqu'ils sont détectés par les analyseurs de sécurité Web standard. Ces points clarifient le comportement attendu et fournissent des conseils pour la conformité de la sécurité :

Confirmation de comportement attendu

Le port TCP 8443 sur Cisco Expressway-E est un point d'extrémité de service/API HTTPS qui n'est pas destiné à l'accès par navigateur générique ou à l'analyse de service Web standard. Lorsque les analyseurs de sécurité envoient des requêtes génériques ou non valides à ce port, ils peuvent recevoir des réponses qui n'incluent pas tous les en-têtes de sécurité HTTP. Ce comportement est attendu et prévu.

En-têtes de sécurité dans les réponses HTTPS valides

Cisco Expressway-E inclut les en-têtes de sécurité appropriés dans les réponses API HTTPS valides et les interactions de service légitimes. Les en-têtes sont présents lorsque l'accès au port est effectué correctement par le biais d'appels API appropriés ou lors de flux d'authentification valides tels que les processus de connexion Webex. Vérifiez cela en collectant des journaux de diagnostic à partir de l'Expressway.

Exemple d'en-têtes de sécurité présents dans une réponse HTTPS valide sur le 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
```

Exemple d'en-têtes de sécurité dans la réponse API sur le 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
```

Exemple de réponse du scanner

Lorsque des scanners génériques ou des requêtes curl sont effectuées sur le port 8443 sans contexte API approprié, ils reçoivent une réponse 400 Bad Request avec des en-têtes limités. Le port TCP 8443 n'est pas destiné à être accédé (par exemple par un navigateur), sauf via des requêtes 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
```

Configuration des en-têtes de sécurité

Les en-têtes de sécurité HTTP ne sont pas configurables par l'utilisateur sur Cisco Expressway-E. Ces en-têtes sont entièrement contrôlés par le logiciel Expressway et sont inclus automatiquement dans les réponses appropriées en fonction du type de demande et d'interaction de service.

Motif

Le port TCP 8443 de Cisco Expressway-E est conçu comme un point d'extrémité API HTTPS pour des communications de service spécifiques, et non comme un port de service Web standard accessible via des requêtes HTTP génériques. Les scanners de sécurité qui envoient des requêtes génériques ou non valides à ce port reçoivent 400 réponses de requêtes incorrectes qui n'incluent pas l'ensemble des en-têtes de sécurité HTTP. Ce comportement est documenté dans l'ID de bogue Cisco CSCvt86137, où les développeurs ont déterminé que l'importance des en-têtes de sécurité dépend du contenu rendu, et l'Expressway utilise déjà des en-têtes de sécurité le cas échéant.

Le manque d'en-têtes dans les réponses de l'analyseur représente le comportement attendu du produit plutôt qu'une vulnérabilité de sécurité, car les en-têtes sont présents dans les interactions API légitimes et les flux de services.

Autres informations utiles

- Guide de configuration de l'utilisation des ports IP Cisco Expressway - Accès mobile et à distance
- ID de bogue Cisco CSCvt86137 - En-têtes de sécurité dans les réponses HTTP d'Expressway
- ID de bogue Cisco CSCvx01616 - En-tête Strict-Transport-Security dans les réponses de l'analyseur de port
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.