Intestazioni di sicurezza HTTP Expressway-E sulla porta 8443 - Comportamento previsto e falsi positivi dello scanner di sicurezza

Sommario

Problema

Gli scanner di vulnerabilità della sicurezza segnalano intestazioni di sicurezza HTTP mancanti durante l'analisi di Cisco Expressway-E sulla porta TCP 8443. La valutazione della protezione indica che le intestazioni di protezione HTTP mancano e sono contrassegnate per il monitoraggio e l'aggiornamento:

- Content-Security-Policy
- Policy-Embedder-Cross-Origin
- Criteri di apertura incrociati
- Criteri risorse incrociati
- Criteri di autorizzazione
- Referrer-Policy
- Strict-Transport-Security
- Opzioni X-Content-Type
- Opzioni X-Frame
- Protezione X-XS

Le organizzazioni devono capire se queste intestazioni possono essere configurate manualmente su Cisco Expressway-E o se rappresentano il comportamento previsto del prodotto, una limitazione o un difetto noto che richiede la correzione per motivi di conformità alla sicurezza.

Ambiente

- Cisco Expressway-E
- Apri la porta TCP 8443 analizzata dallo scanner di porta (ad esempio ambiente di accesso remoto e mobile)

Risoluzione

Le intestazioni di sicurezza HTTP mancanti sulla porta TCP 8443 rappresentano il comportamento previsto di Cisco Expressway-E e devono essere considerate un falso positivo quando rilevate dagli scanner standard per la sicurezza Web. Questi punti chiariscono il comportamento previsto e forniscono orientamenti per la conformità in materia di sicurezza:

Conferma comportamento previsto

La porta TCP 8443 su Cisco Expressway-E è un endpoint di servizio/API HTTPS non progettato per l'accesso al browser generico o per l'analisi di servizi Web standard. Quando gli scanner di sicurezza inviano richieste generiche o non valide a questa porta, possono ricevere risposte che non includono tutte le intestazioni di sicurezza HTTP. Questo comportamento è previsto e previsto.

Intestazioni di sicurezza in risposte HTTPS valide

Cisco Expressway-E non include le intestazioni di sicurezza appropriate in risposte valide all'API HTTPS e interazioni di servizio legittime. Le intestazioni sono presenti quando si accede correttamente alla porta tramite le chiamate API appropriate o durante i flussi di autenticazione validi, ad esempio i processi di accesso Webex. Per verificarlo, raccogliere i log di diagnostica da Expressway.

Esempio di intestazioni di sicurezza presenti in una risposta HTTPS valida sulla 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
```

Esempio di intestazioni di sicurezza nella risposta API sulla porta 43:

```
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
```

Esempio di risposta dello scanner

Quando si inviano scanner generici o richieste curl alla porta 8443 senza un contesto API appropriato, viene ricevuta una risposta di tipo 400 Richiesta non valida con intestazioni limitate. la porta TCP 8443 non è progettata per essere utilizzata (ad esempio da un browser) tranne che tramite richieste 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
```

Configurazione intestazione di sicurezza

Le intestazioni di sicurezza HTTP non sono configurabili dall'utente in Cisco Expressway-E. Queste intestazioni sono controllate interamente dal software Expressway e vengono incluse automaticamente nelle risposte appropriate in base al tipo di richiesta e all'interazione del servizio.

Causa

La porta TCP 8443 su Cisco Expressway-E è progettata come endpoint API HTTPS per comunicazioni di servizio specifiche e non come porta di servizio Web standard accessibile tramite richieste HTTP generiche. Gli scanner di sicurezza che inviano richieste generiche o non valide a questa porta ricevono 400 risposte di richiesta non valida che non includono il supporto completo delle intestazioni di sicurezza HTTP. Questo comportamento è documentato nell'ID bug Cisco CSCvt86137, in cui gli sviluppatori hanno determinato che il significato delle intestazioni di sicurezza dipende dal contenuto sottoposto a rendering e Expressway utilizza già le intestazioni di sicurezza dove appropriato.

La mancanza di intestazioni nelle risposte dello scanner rappresenta il comportamento previsto del prodotto piuttosto che una vulnerabilità della sicurezza, in quanto le intestazioni sono presenti in interazioni API legittime e flussi di servizi.

Contenuto correlato

- Guida alla configurazione dell'utilizzo della porta IP di Cisco Expressway - Accesso remoto e mobile
- Cisco Bug ID CSCvt86137 - Intestazioni di sicurezza nelle risposte HTTP da Expressway
- Cisco Bug ID CSCvx01616 - Intestazione Strict-Transport-Security nelle risposte dello scanner di porta
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).