ポート8443のExpressway-E HTTPセキュリティヘッダー：想定される動作とセキュリティスキャナの誤検出

内容

問題

セキュリティ脆弱性スキャナは、TCPポート8443でCisco Expressway-Eをスキャンするときに、欠落したHTTPセキュリティヘッダーを報告します。セキュリティアセスメントは、次のHTTPセキュリティヘッダーが見つからず、修復のフラグが付けられていることを示しています。

- コンテンツセキュリティポリシー
- Cross-Origin-Embedder – ポリシー
- クロスオリジンオープナーポリシー
- クロスオリジン – リソースポリシー
- アクセス許可 – ポリシー
- リファラポリシー
- 厳密なトランスポートセキュリティ
- X – コンテンツタイプ – オプション
- X-Frame – オプション
- X-XSS保護

組織は、これらのヘッダーをCisco Expressway-Eで手動で設定できるのか、あるいは予測される製品の動作、制限事項、またはセキュリティコンプライアンスのために修復が必要な既知の不具合のいずれであるかを理解する必要があります。

環境

- Cisco Expressway-E
- ポートスキャナでスキャンされたTCPポート8443を開きます（モバイルおよびリモートアクセス環境など）。

解決方法

TCPポート8443で不足していると報告されているHTTPセキュリティヘッダーは、Cisco Expressway-Eの正常な動作を示しており、標準のWebセキュリティスキャナで検出された場合は誤検出と見なす必要があります。次の点では、予想される動作を明確にし、セキュリティコンプライアンスのガイダンスを提供します。

予想される動作の確認

Cisco Expressway-EのTCPポート8443はHTTPS API/サービスエンドポイントであり、一般的なブラウザアクセスや標準のWebサービススキャンを想定していません。セキュリティスキャナがこのポートに一般的な要求または無効な要求を送信する場合、セキュリティスキャナはすべてのHTTPセキュリティヘッダーを含まない応答を受信する可能性があります。この動作は予期されており、意図的なものです。

有効なHTTPS応答のセキュリティヘッダー

Cisco Expressway-Eでは、有効なHTTPS API応答と正当なサービスのインタラクションに適切なセキュリティヘッダーが含まれています。ヘッダーは、適切なAPI呼び出しを使用してポートに正しくアクセスしたとき、またはWebexログインプロセスなどの有効な認証フローの間に存在します。これを確認するには、Expresswayから診断ログを収集します。

ポート8443の有効なHTTPS応答に含まれるセキュリティヘッダーの例：

```
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
```

ポート443のAPI応答のセキュリティヘッダーの例：

```
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
```

スキャナ応答の例

適切なAPIコンテキストなしで汎用スキャナまたはcurl要求がポート8443に対して行われると、ヘッダーが制限された「400 Bad Request」応答が受信されます。TCPポート8443は、API要求を介さない限り、（ブラウザなどによって）アクセスされることを意図していません。

```
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
```

セキュリティヘッダーの設定

HTTPセキュリティヘッダーは、Cisco Expressway-E上でユーザが設定することはできません。これらのヘッダーはExpresswayソフトウェアによって完全に制御され、要求とサービスの相互作用のタイプに基づいて適切な応答に自動的に含まれます。

原因

Cisco Expressway-EのTCPポート8443は、一般的なHTTP要求でアクセス可能な標準のWebサービスポートとしてではなく、特定のサービス通信用のHTTPS APIエンドポイントとして設計されています。このポートに一般的な要求または無効な要求を送信するセキュリティスキャナは、HTTPセキュリティヘッダーの完全な補完を含まない400個のBad Request応答を受信します。この動作は、Cisco Bug ID CSCvt86137に記載されています。この不具合は、開発者がセキュリティヘッダーの重要性がレンダリングされるコンテンツに依存すると判断し、Expresswayが必要に応じてすでにセキュリティヘッダーを使用している場合に発生します。

スキャナ応答にヘッダーが含まれていないことは、正規のAPIインタラクションやサービスフローにヘッダーが含まれるため、セキュリティの脆弱性ではなく、製品の期待される動作を表しています。

関連コンテンツ

- Cisco Expressway IPポート使用設定ガイド – モバイルおよびリモートアクセス
- Cisco Bug ID CSCvt86137 - ExpresswayからのHTTP応答のセキュリティヘッダー
- Cisco Bug ID CSCvx01616 – ポートスキャナ応答のStrict-Transport-Securityヘッダー
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。