Cisco Secure Web Applianceのコンテンツエンコーディングフィルタバイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-wsa-bypass-vXvqwzsj
CVE-2023-20215
初公開日 : 2023-08-02 16:00
最終更新日 : 2024-08-14 14:27
バージョン 1.3 : Final
CVSSスコア : 5.8
回避策 : No workarounds available
Cisco バグ ID : CSCwf55917 CSCwf60901 CSCwf94501

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

Cisco Secure Webアプライアンス(WSA)用Cisco AsyncOSソフトウェアのスキャンエンジンの脆弱性により、認証されていないリモートの攻撃者が設定されたルールをバイパスし、ブロックすべきだったネットワークへのトラフィックを許可する可能性があります。

この脆弱性は、特定のコンテンツ形式でエンコードされた悪意のあるトラフィックの検出が不適切なことに起因します。攻撃者は、該当デバイスを使用して悪意のあるサーバに接続し、巧妙に細工されたHTTP応答を受信することにより、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は明示的なブロックルールをバイパスし、デバイスによって拒否されるはずのトラフィックを受信できるようになります。

この脆弱性に対処する回避策はありません。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj

該当製品

脆弱性のある製品

この脆弱性の公開時点では、Cisco Secure Web Applianceの仮想バージョンとハードウェアバージョンの両方で、deflate、lzma、またはbrotliのコンテンツエンコーディングタイプが有効で

あった場合に、この脆弱性の影響を受けました。

注：Cisco Secure Web Applianceリリース14.5.1以前では、deflateコンテンツエンコーディングタイプはデフォルトで無効になっていますが、lzmaおよびbrotliコンテンツエンコーディングタイプはデフォルトで有効になっています。Cisco Secure Web Applianceリリース14.5.2以降では、deflate、lzma、およびbrotliのcontent-encodingタイプはデフォルトで無効になっています。

コンテンツエンコーディングの種類の決定

Cisco Secure Webアプライアンスでdeflate、lzma、またはbrotliコンテンツエンコーディングタイプが有効になっているかどうかを確認するには、CLIで管理者としてadvancedproxyconfigコマンドを実行し、続いてCONTENT-ENCODINGコマンドを実行します。CONTENT-ENCODINGコマンドがCurrently allowed content-encoding type(s)の下のdeflate、lzma、または br を返す場合、次の例に示すように、そのcontent-encoding typeは有効です。

```
<#root>

cisco-wsa>

advancedproxyconfig


cisco-wsa>

CONTENT-ENCODING


Enter values for the CONTENT-ENCODING options:
Currently allowed content-encoding type(s):

deflate, lzma, br
```

公開時点で脆弱性が確認されている Cisco ソフトウェアのリリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

脆弱性を含んでいないことが確認された製品

このアドバイザリの脆弱性のある製品セクションに記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- セキュアEメールゲートウェイ(旧称：Eメールセキュリティアプライアンス(ESA))：仮想アプライアンスとハードウェアアプライアンスの両方

- 安全な電子メールと Web マネージャ、仮想アプライアンスとハードウェアアプライアンスの両方

注：シスコポートフォリオの簡素化の一環として、セキュリティ製品の名称を変更し、Cisco Secure というブランド名に統一しています。詳細については、「Cisco Secure が登場」を参照してください。

回避策

この脆弱性に対処する回避策はありません。ただし、管理者は次の2つの方法のいずれかで、この脆弱性を緩和できます。

- 必要でない場合は、deflate、lzma、およびbrotliの各コンテンツエンコーディングタイプを無効にします。
- Cisco Secure Web Applianceリリース14.5.2に移行します。このリリースでは、deflate、lzma、およびbrotliのコンテンツエンコーディングタイプはデフォルトで無効になっています。

Content-Encodingタイプの無効化

特定のコンテンツエンコードタイプを無効にするには、次の手順に従います。

1. デバイスの管理コンソールインターフェイスにログインします。
2. advancedproxyconfig > CONTENT-ENCODINGの順に選択します。
3. 特定のコンテンツエンコードタイプに関連付けられている番号を入力します。
4. 次のメッセージが表示されたら、プロンプトでYと入力します。

   <#root>

   ```
   The encoding type <"content-encoding type"> is currently allowed
   Do you want to block it? [N]>
   ```

   Y

   次のメッセージが表示されたら、プロンプトでNと入力します。

   <#root>

   ```
   The encoding type <"content-encoding type"> is currently blocked
   Do you want to allow it? [N]>
   ```

   N

5. Commitコマンドを実行します。

この緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォー

マンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

修正済みソフトウェア

ソフトウェアのアップグレードを検討する際には、シスコ セキュリティ アドバイザリ ページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性とアップグレード ソリューション一式を確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

修正済みリリース

発行時点では、次の表に記載されているリリース情報は正確でした。 最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

左側の列にはシスコソフトウェアリリース、右側の列にはリリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含むリリースが示されています。

Cisco AsyncOS for Secure Web Applianceソフトウェアリリース	First Fixed Release（修正された最初のリリース）
14.0 以前	修正済みリリースに移行。
14.5	14.5.3-033
15.0	15.0 MR（2024 年 8 月）
15.1	修正済みリリースに移行。
15.2	15.2.0-164

Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）は、このアドバイザリに記載されている該当するリリース情報と修正されたリリース情報のみを検証します。

不正利用事例と公式発表

Cisco PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例やその公表は確認しておりません。

出典

シスコは、この脆弱性を報告していただいたq.beyond AG社に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-vXvqwzsj

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.3	修正リリースを更新。	修正済みリリース	Final	2024年8月14日
1.2	リリース固有のデフォルト設定と緩和情報を更新。	「脆弱性のある製品」、「回避策」	Interim	2023 年 11 月 17 日
1.1	ソース情報を更新。	出典	Interim	2023年8月3日
1.0	初回公開リリース	—	Interim	2023 年 8 月 2 日

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

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。