Cisco Secure Email Gateway における任意ファイル書き込みの脆弱性

アドバイザリーID : cisco-sa-esa-afw-bGG2UsjH
初公開日 : 2024-07-17 16:00
バージョン 1.0 : Final
CVSSスコア : 9.8
回避策 : No workarounds available
Cisco バグ ID : CSCwj53998

CVE-2024-20401

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 Email Gateway のコンテンツスキャンおよびメッセージフィルタ処理機能における脆弱性により、認証されていないリモート攻撃者が、基盤となるオペレーティングシステム上の任意のファイルを上書きできる可能性があります。

この脆弱性は、ファイル分析とコンテンツフィルタが有効になっている場合の電子メール添付ファイルの不適切な処理に起因します。細工されたファイルが添付された電子メールが該当デバイスを使用して送信されると、この脆弱性がエクスプロイトされ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、基盤となるオペレーティングシステム上の任意のファイルを置き換えることができる可能性があります。その後、攻撃者は、当該デバイスで、「root」権限を持つユーザーを追加したり、デバイス設定を変更したり、任意のコードを実行したり、永続的なサービス妨害（DoS）状態を引き起こす可能性があります。

注：サービス妨害（Dos）状態から復旧するには、手動による操作が必要です。この状況のデバイスの復旧については、Cisco Technical Assistance Center（TAC）にお問い合わせください。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。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-esa-afw-bGG2UsjH

該当製品

脆弱性のある製品

この脆弱性の影響を受けるのは、Cisco Secure Email Gateway で脆弱性のある Cisco AsyncOS リリースが実行されており、次の両方の条件を満たしている場合です。

- ファイル分析機能（Cisco Advanced Malware Protection（AMP）に含まれる）またはコンテンツフィルタ機能が有効になっていて、着信メールポリシーに割り当てられている。
- コンテンツスキャナツールのバージョンが 23.3.0.4823 より前である。

脆弱性が存在する Cisco ソフトウェア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。

ファイル分析が有効かどうかの確認方法

ファイル分析が有効になっているかどうかを確認するには、次の手順を実行します。

1. 製品の Web 管理インターフェイスに接続します。
2. [メールポリシー（Mail Policies）] > [着信メールポリシー（Incoming Mail Policies）] > [Cisco Advanced Malware Protection] を選択します。
3. いずれかのメールポリシーを選択し、[ファイル分析を有効にする（Enable File Analysis）] の値を調べます。

このチェックボックスをオンにすると、ファイル分析が有効になります。

コンテンツフィルタが有効かどうかの確認方法

コンテンツフィルタが有効になっているかどうかを確認するには、次の手順を実行します。

1. 製品の Web インターフェイスに接続します。
2. [メールポリシー（Mail Policies）] > [着信メールポリシー（Incoming Mail Policies）] > [コンテンツフィルタ（Content Filters）] を選択します。

[コンテンツフィルタ（Content Filters）] 列に [無効（Disabled）] 以外の値が含まれている場合は、コンテンツフィルタが有効になっています。

コンテンツスキャナツールのバージョンの確認方法

実行中のコンテンツスキャナのバージョンを確認するには、CLI コマンド contentscannerstatus を使用します。次の例は、脆弱性のあるバージョンのコンテンツスキャナツールを示しています。

```
<#root>

cisco-esa>
```

```
contentscannerstatus

Component              Version                 Last Updated
Content Scanner Tools  23.1.0.4619.13.0.1500022 Never updated
```

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。

- Cisco Secure Email and Web Manager
- Cisco Secure Web Appliance

回避策

この脆弱性に対処する回避策はありません。

修正済みソフトウェア

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

Cisco.com の シスコサポート & ダウンロードページには、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス（My Devices）] ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。

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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

この脆弱性の修正は、コンテンツ スキャナ ツール パッケージの更新バージョンを通じて配布されています。コンテンツ スキャナ ツール バージョン 23.3.0.4823 以降には、この脆弱性の修正が含まれています。

コンテンツスキャナツールの更新バージョンは、Cisco AsyncOS for Cisco Secure Email Software リリース 15.5.1-055 以降にはデフォルトで含まれています。

コンテンツスキャナツールの更新

コンテンツスキャナツールの更新では、ソフトウェアのアップグレードや製品の再起動は必要ありません。コンテンツスキャナツールの自動更新を設定している場合は、この脆弱性に対処するアクションを実行する必要がない可能性があります。

手動更新

コンテンツスキャナツールを手動で更新するには、次の例に示すように、コマンド CLI contentcannerupdate を使用します。

```
<#root>

cisco-esa>

contentscannerupdate
```

```
Requesting check for new Content Scanner updates.
```

現在のバージョンを確認する方法については、このアドバイザリの「脆弱性のある製品」セクションを参照してください。

自動更新

自動更新を有効にするには、Web 管理インターフェイスで次の手順を実行します。

1. [セキュリティサービス（Security Services）] > [サービスの更新（Service Updates）] を選択します。
2. [更新設定を編集（Edit Update Settings）] をクリックします。
3. [自動更新（Automatic Updates）] チェックボックスをクリックします。
4. [Submit] をクリックします。
5. ページの右上にある [変更の確定（Commit Changes）] を選択します。
6. [変更の確認（Commit Changes）] をクリックすることにより、確定されていない変更を確認します。

Cisco Secure Email Cloud Gateway を使用している場合、アクションは必要ありません。シスコでは、この脆弱性からインフラストラクチャを保護するアクションを実行しており、環境の標準アップグレードプロセスの一環として、コンテンツスキャナツールの修正バージョンが展開されます。

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

この脆弱性は Cisco TAC サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-afw-bGG2UsjH

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2024 年 7 月 17 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。