

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



Advisory ID : cisco-sa-esa-afw-zqYJkjpg

[CVE-2026-](#)

初公開日 : 2026-10-14 16:00

[76519](#)

バージョン 1.0 : Final

CVSSスコア : [9.8](#)

回避策 : No workarounds available

Cisco Bug ID : [CSCwu56223](#)

日本語の情報は原文の英語の非公式な翻訳です。日本語と英語のバージョンに相違がある場合は、英語のバージョンが優先されます。

概要

Cisco Secure Email Gatewayの高度なマルウェア防御(AMP)機能の脆弱性により、認証されていないリモートの攻撃者が基盤となるオペレーティングシステムに任意のファイルを書き込む可能性があります。

この脆弱性は、ファイルレピュテーションサービスが有効な場合の電子メールの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でルート権限を使用して任意のファイルに書き込みを行い、コマンドを実行できる可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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-zqYJkjpg>

Cisco Secure Email Gatewayの改善点と修正プログラムの詳細については、『[Cisco Secure Email GatewayおよびSecure Email and Web Managerのセキュリティ強化リリース : 2026年9月](#)』を参照してください。

該当製品

脆弱性のある製品

この脆弱性は、Cisco Secure Email Gatewayで脆弱性のあるCisco AsyncOSソフトウェアリリ

ースが実行されており、次の両方の条件が満たされている場合に、物理と仮想の両方に影響を与えます。

- Cisco AMPの一部であるファイルレピュテーションサービスが有効になり、メールポリシーに割り当てられます。
- コンテンツスキャナツールのバージョンが25.3.0.5525よりも前である。

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。

ファイルレピュテーションサービスが有効になっているかどうかの確認

ファイルレピュテーションが有効になっているかどうかを確認するには、次の手順に従います。

1. 製品のWebベースの管理インターフェイスに接続します。
2. Mail Policies > Incoming Mail Policies > Advanced Malware ProtectionまたはMail Policies > Outgoing Mail Policies > Advanced Malware Protectionを選択します。
3. メールポリシーを選択し、Enable File Reputationチェックボックスをチェックします。

このチェックボックスをオンにすると、ファイルレピュテーションが有効になります。

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ツールのバージョンを確認するには、CLIで contentscannerstatus コマンドを使用します。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	25.2.0.5427.15.5.001	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

セキュリティ侵害の指標

この脆弱性の不正利用が試行されたことを確認するには、次のコマンドを使用してsystem_logsを確認します。

```
<#root>

esa-appliance>

grep "System Security" system_logs
```

デバイスがクラスターの一部である場合、各クラスターデバイスのログを確認します。

次の表に示すログメッセージの1つが出力に表示される場合があります。次の手順については、対応する「推奨処置」の列を参照してください。

ログ メッセージ	推奨処置
システムセキュリティ：セキュリティ侵害が疑われるインジケータが見つかりました。さらに詳しい推奨事項については、TACにお問い合わせください。	侵入が検出されました。このセキュリティアドバイザリの「 推奨事項 」セクションの指示に従ってください
システムセキュリティ：セキュリティスキャンは完了しませんでした。さらに詳しい推奨事項については、TACにお問い合わせください。	サポートの詳細については、Cisco Technical Assistance Center(TAC)にお問い合わせください。
システムセキュリティ：セキュリティ侵害インジケータが見つかりませんでした。	セキュリティ侵害は検出されませんでした。該当する場合は、修正済みのソフトウェアリリースにアップグレードします

Cisco Secure Email Cloud では、CLI アクセス権を持たない管理者は、前述の侵害の兆候を個別に確認できない場合があります。シスコは、悪意のあるアクティビティが検出された Cisco Secure Email Cloud デバイスを所有するお客様に直接連絡を取りました。

注：この脆弱性の不正利用に成功すると、攻撃者はroot権限でコマンド実行を取得する可能性があります。このアクセスレベルでは、攻撃者は悪用の証拠や侵入の痕跡を削除したり、隠したりできます。シスコでは、影響を受けるデバイスの外部にあるネットワークログとファイアウォールログを照合して、疑わしい動作（影響を受けるデバイスから外部IPアドレスへの予期しないアップロードや、悪意のあるIPアドレスからのダウンロードなど）を特定することを強く推奨します。

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

シスコでは、回避策や緩和策（該当する場合）は、修正済みソフトウェアリリースへのアップグレードが利用可能になるまでの一時的な解決策であると考えています。この脆弱性を修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

修正リリース

次の表では、左の列にシスコ ソフトウェアリリースを記載しています。右側の列は、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最初のリリースを示しています。このセクションの表に記載されている適切な修正済みソフトウェアリリースにアップグレードすることをお勧めします。

Cisco Secure Email Gateway向けCisco AsyncOSソフトウェアリリース	第 1 修正済みリリース
15.5	15.5.5-014
16.0	修正済みリリースに移行。
16.5	16.5.0-780

リリース16.5より前のCisco AsyncOSソフトウェアリリースを実行している場合は、リリース16.5.0-780に移行することを強く推奨します。

この脆弱性に対する修正は、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、ライセンスおよびサポートされているすべてのCisco AsyncOSソフトウェアリリースにも配布されます。コンテンツ スキャナ ツール バージョン 25.3.0.5525 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

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有効にしている場合は、更新の適用後に何らかの措置を講じる必要はありません。自動更新を無効にしているお客様は、コンテンツスキャナツールの更新を手動で適用する必要があります。

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、CLIでコマンド

contentscannerupdate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](#)」の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ベースの管理インターフェイスで次の手順を実行します。

1. Security Services > Service Updatesの順に選択します。
2. Edit Update Settingsをクリックします。
3. 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Commit Changesを選択します。
6. Commit Changesをクリックして、コミットされていない変更を確定します。

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ための対策を講じています。また、この環境の標準的なアップグレードプロセスの一部として、すでに修正済みバージョンのコンテンツスキャナツールが導入されています。

シスコの 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済みリリース情報のみを検証します。

推奨事項

オンプレミスの物理デバイス

物理アプライアンスでエクспロイトが疑われる場合、シスコでは、[Cisco Technical Assistance Center \(TAC \)](#) に連絡し、さらなるサポートを受けることを推奨しています。侵害の可能性に関する調査を迅速に進めるため、該当するアプライアンスでリモートアクセスが有効になっていることを確認してください。詳細なガイダンスについては、「[Cisco ESA/WSA/SMA でのリモートアクセスに関する FAQ](#)」を参照してください。

オンプレミスの仮想デバイス

仮想アプライアンスでエクスプロイトが疑われる場合、シスコでは、可能な場合、以下のアクションにより、デバイスを安全な設定に復元することを強く推奨しています。

1. お客様のインシデント対応ポリシーに記載されているとおり、フォレンジック情報を維持します。重要：以下のいずれかの手順に進む前に、フォレンジック情報を記録しておいてください。侵害されたインスタンスをアップグレードすると、フォレンジックデータとログが破壊されます。
2. 修正済みソフトウェアリリースのいずれかを実行する新しい仮想マシンを展開します。
3. 以前の設定ファイルをインポートせずに、製品の設定を再構築します。
4. アプライアンスにインストールされているログイン情報および暗号資料を更新します。
5. システムに異常な動作がないか引き続き監視します。

注：Cisco Secure Email Gateway アプライアンスは、クラスタの一部にすることができます。SSH キーペアは、クラスタメンバー間の認証に使用されます。この脆弱性のエクスプロイトが成功すると、侵害されたアプライアンス上で、この通信に使用される SSH 秘密キーにアクセスできる可能性があります。これらのキーにアクセスすることで、攻撃者は他のクラスタメンバーを侵害できる可能性があります。このため、侵害されたアプライアンスが 1 台以上含まれているクラスタについては、各メンバーを安全な設定に復元することを強く推奨します。

アプライアンスを復元できない場合は、[Cisco TAC](#) に連絡し、さらなるサポートを受けることを推奨しています。

エクスプロイトの疑いがなく、デバイスで該当のソフトウェアリリースが実行されている場合、シスコは修正済みのリリースにアップグレードすることを強く推奨します。

Cisco Secure Email Cloud

シスコは、Cisco Secure Email Cloud に属するデバイスについて、徹底的な脅威インテリジェンス調査を実施しました。シスコは、侵害の可能性を示す兆候が確認された Cisco Secure Email Cloud デバイスを所有するお客様に直接連絡を取りました。シスコでは、修復およびリカバリ操作に取り組んでいます。シスコは、自社の管理下にある緩和策をすでに展開しています。

また、連絡を受けたお客様には、可能であれば、アプライアンスにインストールされているログイン情報および暗号資料を更新して、デバイスを安全な設定に復元することを強く推奨します。

さらに、アプライアンスへのアクセスを制限し、堅牢なアクセス制御メカニズムを実装することを強く推奨します。

セキュリティ強化のための一般的な推奨事項

- アプライアンスを Cisco AsyncOS ソフトウェアの最新バージョンにアップグレードします。

- インターネットからアプライアンスへのアクセスを防止します。アプライアンスにインターネットアクセスが必要な場合、ユーザーガイドに記載されているポートおよびプロトコル上の既知の信頼できるホストのみにアプライアンスアクセスを制限します。
- Cisco Secure Email Gateway の場合、メールと管理機能を個別のネットワーク インターフェイスに分離します。これにより、不正なユーザーが内部の管理ネットワークにアクセスする可能性が低減されます。詳細については、デバイスのユーザーガイドを参照してください。
- ファイアウォールなどのフィルタリングデバイスの背後に Cisco Secure Email Gateway および Cisco Secure Email and Web Manager アプライアンスを配置して保護し、アプライアンスとの間の管理トラフィックをフィルタリングする一方で、既知の信頼できるホストのみがアプライアンスにトラフィックを送信できるようにします。2 層ファイアウォールの使用によって、ネットワークプランニングの柔軟性が高まり、エンドユーザーが外部 DMZ に直接接続することを防止できます。[Cisco Secure Email Gateway](#) および [Cisco Secure Email and Web Manager](#) 向けユーザーガイドの「デプロイメント」セクションを参照してください。
- ログトラフィックを定期的に監視して、アプライアンスとの間の予期しないトラフィックがないかどうかを調べます。可能であれば、ログは外部サーバーに送信し、十分なログデータを使用して事後調査を実行できるように十分な期間にわたって保持する必要があります。
- メイン管理者ポータル の HTTP を無効にします。
- HTTP や FTP などの不要なネットワークサービスを無効にします。特定のサービス機能の詳細については、Cisco Secure Email Gateway および Cisco Secure Email and Web Manager のユーザーガイドを参照してください。
- アプライアンスへのエンドユーザー認証には、SAML や Lightweight Directory Access Protocol (LDAP) などの強力な形式を使用します。より安全な認証方法については、「[スパム管理機能にアクセスするエンドユーザーの認証オプション](#)」を参照してください。
- デフォルトの管理者パスワードを、より安全なパスワードに変更します。必要なアクセス要件に基づいてユーザ アカウントを作成し、管理者アカウントへのアクセスを制限する。また、すべての管理者に対してオペレータ アカウントを作成します。
- SSL/TLS を使用し、認証局 (CA) から SSL 証明書を取得するか、または自己署名証明書を作成します。

関連リソース

次のリソースは、影響を受けたアプライアンスを安全な状態に復元するのに役立ちます。一部のドキュメントは特定の製品に関連していますが、手順はほとんど互換性があります。手順について具体的な質問がある場合は、[Cisco TAC にお問い合わせください](#)。

交換用の仮想アプライアンスをダウンロードするには、関連するシスコのソフトウェア ダウンロード ページにアクセスします。

- [Cisco Secure Email Gateway](#)
- [Cisco Secure Email and Web Manager](#)

詳細については、『[User Guide for AsyncOS 16.5 for Cisco Secure Email and Web Manager](#)』を参照してください。次のセクションを参照してください。

- アプライアンスからのレポートデータのエクスポートについては、「[Working with Reports](#)」を参照してください。
- 隔離中のメッセージを削除する方法については、「[Spam Quarantine](#)」を参照してください。
- 追加情報については、「[Centralizing Policy, Virus, and Outbreak Quarantines](#)」を参照してください。

不正利用事例と公式発表

2026年10月、Cisco PSIRTはこの脆弱性が活発に悪用されていることを認識しました。

送信元

この脆弱性は内部セキュリティスキャンで発見されました。

URL

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

改訂履歴

バージョン	説明	セクション	Status	日付
1.0	初版リリース	—	Final	2026年10月14日

利用規約

ソフトウェアのダウンロードおよびテクニカルサポート

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。お客様がソフトウェアをダウンロードできるのは、シスコから直接、あるいはシスコ認定再販業者やシスコ認定パートナーを通じて調達されたもので、ライセンスが有効なものに限ります。

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](#)

[Technical Assistance Center \(TAC \)](#) 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。

[ソフトウェアのアップグレードを検討する](#) 際には、関連するシスコ製品の[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。

利用規約の詳細

シスコは、商品適格性または特定目的への適合性に関する保証を含め、明示的か黙示的かを問わず、いかなる種類の保証も表明しません。前述の一般論に限定されることなく、シスコは、本情報の正確性または完全性を保証するものではありません。コンテンツは「現状のまま」提供されます。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。

本セキュリティアドバイザリに含まれる情報のコピーや要約には、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。本セキュリティアドバイザリの最新版については、[シスコ セキュリティ アドバイザリ](#) ページをご覧ください。Cisco 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済みリリース情報のみを評価します。詳細については、[シスコのセキュリティ脆弱性ポリシー](#)を参照してください。

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。