Cisco Secure Email and Web Manager、Secure Email Gateway、およびSecure Web Applianceの脆弱性

Medium

アドバイザリーID : cisco-sa-esa-sma-wsa-multi-yKUJhS34
初公開日 : 2025-02-05 16:00
バージョン 1.0 : Final
CVSSスコア : 6.5
回避策 : No workarounds available
Cisco バグ ID : CSCwk70574 CSCwk70576 CSCwk98506 CSCwk70559 CSCwk70547 CSCwk70590

CVE-2025-20184
CVE-2025-20185

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 and Web Manager、Cisco Secure Email Gateway、およびCisco Secure Web Appliance用のCisco AsyncOSソフトウェアにおける複数の脆弱性により、攻撃者がローカルまたはリモートで任意のコマンドを実行できる可能性があります。

これらの脆弱性の詳細については本アドバイザリの「詳細情報」セクションを参照してください。

シスコはこれら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。これら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-sma-wsa-multi-yKUJhS34

該当製品

脆弱性のある製品

公表時点では、CVE-2025-20184は次のシスコ製品の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に影響を与えていました。

- Secure Email Gateway
- Cisco Secure Web Appliance

公表時点では、CVE-2025-20185は次のシスコ製品の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に影響を与えていました。

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

このアドバイザリの公開時点で脆弱性が存在するシスコ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。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が存在する製品セクションにリストされている製品だけがこれらの脆弱性の影響を受けることが知られています。

シスコは、CVE-2025-20184がCisco Secure Email and Web Managerに影響を与えないことを確認しました。

詳細

これらの脆弱性は依存関係にはなく、いずれかの脆弱性をエクスプロイトするために、他の脆弱性をエクスプロイトする必要はありません。また、いずれかの脆弱性の影響を受けるリリースであっても、他の脆弱性の影響は受けない場合があります。

脆弱性の詳細は以下のとおりです。

CVE-2024-20184:Cisco Secure Email GatewayおよびCisco Secure Web Applianceにおけるコマンドインジェクションの脆弱性

Cisco Secure Email GatewayおよびCisco Secure Web Appliance用のCisco AsyncOSソフトウェアのWebベース管理インターフェイスにおける脆弱性により、認証されたリモートの攻撃者が該当デバイスに対してコマンドインジェクション攻撃を実行できる危険性があります。この脆弱性を不正利用するには、攻撃者は有効な管理者クレデンシャルを持っている必要があります。

この脆弱性は、該当デバイスによるXMLコンフィギュレーションファイルの検証が不十分であることに起因します。攻撃者は、巧妙に細工されたXMLコンフィギュレーションファイルをアップロードすることにより、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、root権限を使用して基盤となるオペレーティングシステムにコマンドを挿入できる可能性があります。

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。

バグID: CSCwk70559、CSCwk70576、CSCwk98506
CVE ID：CVE-2024-20184
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.5
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N

CVE-2024-20185:Cisco Secure Email and Web Manager、Cisco Secure Email Gateway、およびCisco Secure Web Applianceにおける特権昇格の脆弱性

Cisco Secure Email and Web Manager、Cisco Secure Email Gateway、およびCisco Secure Web Appliance用のCisco AsyncOSソフトウェアのリモートアクセス機能の実装における脆弱性により、認証されたローカルの攻撃者が特権をrootに昇格できる危険性があります。この脆弱性を不正利用するには、攻撃者は有効な管理者クレデンシャルを持っている必要があります。

この脆弱性は、リモートアクセス機能のパスワード生成アルゴリズムのアーキテクチャ上の欠陥に起因します。攻撃者は、サービスアカウントの一時パスワードを生成することで、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、攻撃者はルートとして任意のコマンドを実行し、基盤となるオペレーティングシステムにアクセスする可能性があります。

注：攻撃者がアクセスできる情報の範囲は無制限であるため、この脆弱性のSecurity Impact Rating(SIR)は「中」です。

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。

バグID: CSCwk70590、CSCwk70547、CSCwk70574
CVE ID：CVE-2024-20185
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：3.1
CVSSベクトル：CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N

回避策

これら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

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完全なアップグレード ソリューション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

公開時点では、次の表の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。

左の列にはシスコのソフトウェアリリースが、中央の列と右の列には、そのリリースがこのアドバイザリに記載された脆弱性の影響を受けるかどうかと、これら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 Secure Email and Web Manager

Cisco AsyncOS ソフトウェアリリース	CVE-2025-20184 の最初の修正済みリリース	CVE-2025-20185 の最初の修正済みリリース
15.0 以前	脆弱性なし	修正済みリリースに移行。
15.5	脆弱性なし	15.5.3-017
16.0	脆弱性なし	16.0.1-010

Secure Email Gateway

Cisco AsyncOS ソフトウェアリリース	CVE-2025-20184 の最初の修正済みリリース	CVE-2025-20185 の最初の修正済みリリース
15.0 以前	修正済みリリースに移行。	修正済みリリースに移行。
15.5	修正済みリリースに移行。	15.5.3-022
16.0	16.0.0-050	16.0.1-017

Cisco Secure Web Appliance

Cisco AsyncOS ソフトウェアリリース	CVE-2025-20184 の最初の修正済みリリース	CVE-2025-20185 の最初の修正済みリリース
15.1 以前	修正済みリリースに移行。	修正済みリリースに移行。
15.2	15.2.2-009	15.2.2-009

ほとんどの場合、アプライアンスのWebベース管理インターフェイスのシステムアップグレードオプションを使用して、ネットワーク経由でソフトウェアをアップグレードできます。Webベースの管理インターフェイスを使用してデバイスをアップグレードするには、次の手順を実行します。

1. [システム管理（System Administration）] > [システムアップグレード（System Upgrade）] を選択します。
2. [アップグレード（Upgrade）] オプションをクリックします。
3. Download and Installをクリックします。
4. アップグレードするリリースを選択します。
5. [アップグレード準備（Upgrade Preparation）] 領域で、適切なオプションを選択します。
6. [続行（Proceed）] をクリックすると、アップグレードが始まります。アップグレードのステータスを示す経過表示バーが表示されます。

アップグレードが完了すると、デバイスがリブートします。

Cisco Secure Email Cloudには、サービスソリューションの一部として、Cisco Secure Email GatewayとCisco Secure Email & Web Managerデバイスが含まれています。シスコは、このソリューションに含まれる製品について、定期的なメンテナンスを行っています。お客様から Cisco TAC に連絡して、ソフトウェアのアップグレードを要求することもできます。

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とその公表は確認しておりません。

出典

シスコは、これらの脆弱性を報告していただいたExodus Intelligenceに感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-wsa-multi-yKUJhS34

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	2025年2月5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。