Cisco Secure Email and Web ManagerおよびSecure Email Gatewayのクロスサイトスクリプティングの脆弱性

Medium

アドバイザリーID : cisco-sa-esa-sma-xss-WCk2WcuG　CVE-2025-20180
初公開日 : 2025-02-05 16:00
バージョン 1.0 : Final
CVSSスコア : 4.8
回避策 : No workarounds available
Cisco バグ ID : CSCwn25954 CSCwn26371

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(CEM)およびSecure Email Gateway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、インターフェイスのユーザに対してストアドクロスサイトスクリプティング(XSS)攻撃を実行する可能性があります。

この脆弱性は、ユーザー入力の検証が不十分なことに起因します。攻撃者は、細工されたリンクをクリックするように該当インターフェイスのユーザを誘導することで、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、攻撃者は該当インターフェイスのコンテキストで任意のスクリプトコードを実行したり、ブラウザベースの機密情報にアクセスする可能性があります。この脆弱性を不正利用するには、攻撃者は少なくともOperatorロールを持つユーザアカウントの有効なクレデンシャルを持っている必要があります。

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。

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-xss-WCk2WcuG

該当製品

脆弱性のある製品

公開時点では、デバイスの設定にかかわらず、次のシスコ製品で脆弱性が存在するCisco AsyncOSソフトウェアリリースが実行されている場合にこの脆弱性の影響を受けました。

- 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
- Cisco Secure Email Gateway、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

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のある製品セクションにリストされている製品だけがこ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、この脆弱性がCisco Secure Web Appliance（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）には影響を与えないことを確認しました。

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

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 Secure Email and Web Manager

Cisco AsyncOS 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）
15.0 以前	修正済みリリースに移行。
15.5	15.5.3-017
16.0	16.0.1-010

Secure Email Gateway

Cisco AsyncOS 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）
15.0 以前	修正済みリリースに移行。
15.5	15.5.3-022
16.0	16.0.1-017

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やその公表は確認し

ておりません。

出典

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-xss-WCk2WcuG

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。