Cisco Secure Email GatewayおよびCisco Secure Email & Web Managerに対するサイバー攻撃に関するレポート

アドバイザリーID : cisco-sa-sma-attack-N9bf4
初公開日 : 2025-12-17 16:00
バージョン 1.0 : Interim
CVSSスコア : 10.0
回避策 : No workarounds available
Cisco バグ ID : CSCws36549

CVE-2025-20393

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

12月10日、シスコは新しいサイバー攻撃キャンペーンを知りました。このキャンペーンは、インターネットに開いている特定のポートを持つアプライアンスのうち、Cisco AsyncOSソフトウェアfor Cisco Secure Email GatewayおよびCisco Secure Email and Web Managerを実行しているアプライアンスの一部を対象としています。この攻撃により、脅威アクターは、影響を受けるアプライアンスの基盤となるオペレーティングシステム上でroot権限で任意のコマンドを実行できるようになります。調査を続けていることで、侵害されたアプライアンスに対して一定の制御を維持するために、脅威アクターが持続的なメカニズムを仕掛けている証拠が見つかっています。

シスコは、このアドバイザリの推奨事項セクションに記載されているガイダンスに従って、リスクを評価し、リスクを軽減することを強く推奨します。

Cisco Talosはブログ記事「UAT-9686 actively targets Cisco Secure Email Gateway and Secure Email and Web Manager」でこれらの攻撃について説明しています。

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-sma-attack-N9bf4

該当製品

シスコは、この攻撃キャンペーンの調査を続けています。調査の進捗に応じて、より多くの情報が入手可能になり次第、このアドバイザリを更新します。

脆弱性のある製品

この攻撃キャンペーンは、Cisco Secure Email Gateway（物理と仮想の両方）とCisco Secure Email and Web Managerアプライアンス（物理と仮想の両方）に影響を与えます。この影響を受けるのは、次の条件の両方を満たしている場合です。

- アプライアンスにスパム検疫機能が設定されている。
- スパム検疫機能は、インターネットに公開されており、インターネットから到達可能です。

スパム検疫機能は、デフォルトでは有効になっていません。これらの製品の導入ガイドでは、このポートをインターネットに直接公開する必要はありません。

注:Cisco AsyncOSソフトウェアのすべてのリリースが、この攻撃キャンペーンの影響を受けます。

Cisco Secure Email Gatewayアプライアンスでスパム検疫が有効になっているかどうかを確認する

アプライアンスでスパム検疫機能が設定され有効になっているかどうかを確認するには、Web管理インターフェイスに接続し、Network > IP Interfaces > [Select the Interface on the Spam Quarantine is configured]の順にメニューします。スパム検疫の横にあるチェックボックスをオンにすると、この機能が有効になります。

Cisco Secure Email and Web Managerアプライアンスでスパム検疫が有効になっているかどうかを確認する

アプライアンスでスパム検疫機能が設定され有効になっているかどうかを確認するには、Web管理インターフェイスに接続し、管理アプライアンス>ネットワーク > IPインターフェイス> [スパム検疫が設定されているインターフェイスを選択してください]。スパム検疫の横にあるチェックボックスをオンにすると、この機能が有効になります。

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のみが、この攻撃キャンペーンの影響を受けることが分かっています。

シスコは、Cisco Secure Email Cloudの一部であるすべてのデバイスが影響を受けないことを確認しました。

シスコでは、Cisco Secure Webに対するエクスプロイト活動は確認していません。

セキュリティ侵害の痕跡

このアドバイザリで説明されている攻撃キャンペーンの一環として、脅威アクターは、侵害され

たアプライアンスへのリモートアクセスに使用される持続的な秘密のチャネルを仕掛けました。

アプライアンスが侵害されたかどうかを明示的に確認したい場合は、Cisco Technical Assistance Center(TAC)でケースをオープンしてください。潜在的な侵害の調査を迅速に進めるために、影響を受け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、こちらのテクニカルノートを参照してください。

いずれの場合も、このアドバイザリの「推奨事項」セクションに記載されているガイダンスに従うことを強く推奨します。

回避策

この攻撃キャンペーンに関するリスクを直接軽減する回避策は特定されていませんが、管理者はこのアドバイザリの「推奨事項」の項に記載されているガイダンスを参照してその指示に従うことができます。

不正利用事例と公式発表

2025年12月、Cisco Product Security Incident Response Team(PSIRT)は、Cisco Secure Email GatewayおよびCisco Secure Email and Web Managerアプライアンスを対象とした潜在的な悪意のあるアクティビティを検出しました。

出典

この攻撃キャンペーンは、当初、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-sma-attack-N9bf4

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	—	Interim	2025年12月17日

利用規約

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。