Cisco Secure Email and Web Manager、Secure Email Gateway、およびSecure Web Appliance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-wsa-xss-bgG5WHOD
初公開日 : 2024-05-15 16:00
最終更新日 : 2024-06-12 15:37
バージョン 1.1 : Final
CVSSスコア : 6.1
回避策 : No workarounds available
Cisco バグ ID : CSCwe88788 CSCwi59618 CSCwf84882 CSCwf73258 CSCwe91887 CSCwf93368 CSCwj12619

CVE-2024-20256
CVE-2024-20258
CVE-2024-20257
CVE-2024-20383

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 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複数の脆弱性により、Cisco Secure Email and Web Manager、Secure Email Gateway(旧Email Security Appliance(ESA))、およびSecure Web Applianceがリモート攻撃者によってインターフェイスのユーザに対してクロスサイトスクリプティング(XSS)攻撃が実行され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-xss-bgG5WHOD

該当製品

脆弱性のある製品

公表時点で、CVE-2024-20256は次のシスコ製品に影響を与えています。

- 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
- セキュアWebアプライアンス（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）

公開時点では、CVE-2024-20257の影響を受けたCisco Secure Email Gatewayは、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です。

公表時点で、CVE-2024-20258は次のシスコ製品に影響を与えています。

- 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
- セキュアなEメールゲートウェイ（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）

公開時点では、CVE-2024-20383は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のCisco Secure Email and Web Managerに影響を与えていました。

公開時点で脆弱性が確認されている Cisco ソフトウェアの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、CVE-2024-20256が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）に影響を与えないことを確認しました。

シスコは、CVE-2024-20257が次のシスコ製品には影響を与えないことを確認しました。

- 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
- セキュアWebアプライアンス（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）

シスコは、CVE-2024-20258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）に影響を与えないことを確認しました。

シスコは、CVE-2024-20383が次のシスコ製品には影響を与えないことを確認しました。

- セキュアなEメールゲートウェイ（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）
- セキュアWebアプライアンス（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）

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別の脆弱性をエクスプロイトする必要はありません。さらに、いずれかの脆弱性の影響を受けるソフトウェア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-2024-20258: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脆弱性の影響

Cisco Secure Email and Web Manager(SEM)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、認証されていないリモートの攻撃者によってインターフェイスのユーザに対するXSS攻撃が実行される可能性があります。

この脆弱性は、ユーザ入力の不十分な検証に起因します。攻撃者は、細工されたリンクを該当インターフェイスのユーザがクリックするように誘導することで、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。

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: CSCwf84882、CSCwf93368、CSCwj12619
CVE ID：CVE-2024-20258
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.1
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVE-2024-20256:Cisco Secure Email & Web ManagerおよびSecure Web Applianceのストアドクロスサイトスクリプティングの脆弱性

Cisco Secure Email & Web Managerおよび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、そのインターフェイスのユーザに対してXSS攻撃を実行する可能性があります。

この脆弱性は、ユーザ入力の不十分な検証に起因します。攻撃者は、細工されたリンクを該当イ

ンターフェイスのユーザがクリックするように誘導することで、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。

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: CSCwe91887、CSCwe88788
CVE ID：CVE-2024-20256
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：4.8
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N

CVE-2024-20257:Cisco Secure Email Gatewayで保存されたクロスサイトスクリプティングの脆弱性

Cisco Secure Email Gateway用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、ユーザ入力の不十分な検証に起因します。攻撃者は、細工されたリンクを該当インターフェイスのユーザがクリックするように誘導することで、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。

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:CSCwf73258
CVE ID：CVE-2024-20257
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：4.8
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N

CVE-2024-20383:Cisco Secure Email and Web Managerのストアドクロスサイトスクリプティングの脆弱性

Cisco Secure Email and Web Manager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、ユーザ入力の不十分な検証に起因します。攻撃者は、細工されたリンクを該当イ

ンターフェイスのユーザがクリックするように誘導することで、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。

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:CSCwi59618
CVE ID：CVE-2024-20383
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：4.8
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/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。

修正済みリリース

このドキュメントの発行時点では、次の表に示す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Ciscoソフトウェアリリースが、右の列にはそのリリースが本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、またどのリリースにこれらの脆弱性に対する修正が含まれているかを示します。

Cisco Secure Email and Web Manager

Cisco AsyncOS 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	15.5.1-024

セキュアEメールゲートウェイ

Cisco AsyncOS リリース	First Fixed Release（修正された最初のリリース）
14.3 以前	修正済みリリースに移行。
15.0	15.0.2-034
15.5	15.5.1-055

Cisco Secure Web Appliance

Cisco AsyncOS リリース	First Fixed Release（修正された最初のリリース）
14.0 以前	修正済みリリースに移行。
14.5	14.5.2-011
15.0	15.0.0-355

ほとんどの場合、アプライアンスのWebインターフェイスで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 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. [アップグレードオプション（Upgrade Options）] をクリックします。
3. [ダウンロードしてインストール（Download and Install）] を選択します。
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）] をクリックして、アップグレードを開始します。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 Gateway（旧Cisco Cloud Email Security）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 and 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。お客様は、シスコサポート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

CVE-2024-20257：この脆弱性は、シスコのRoberto Petrillo氏が社内セキュリティテストで発見しました。

CVE-2024-20256およびCVE-2024-20258：これらの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たものです。

CVE-2024-20383：この脆弱性を報告していただいたBastion Security Group(BSG)のAhmad Ashraff氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-wsa-xss-bgG5WHOD

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	Cisco Secure Email Gateway 15.0トレインの修正済みリリースを追加。	修正済みリリース	Final	2024年6月12日
1.0	初回公開リリース	—	Final	2024 年 5 月 15 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。