Cisco EメールセキュリティアプライアンスおよびCisco Secure EメールおよびWeb Managerの脆弱性

High

アドバイザリーID : cisco-sa-esa-sma-privesc-9DVkFpJ8

初公開日 : 2023-02-15 16:00

最終更新日 : 2023-02-16 17:32

バージョン 1.1 : Final

CVSSスコア : 6.5

回避策 : No workarounds available

Cisco バグ ID : CSCwd50043 CSCwd29905 CSCwd29901

CVE-2023-20009

CVE-2023-20075

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 Eメールセキュリティアプライアンス(ESA)およびCisco Secure Email and Web ManagerのWeb UIおよびCLIにおける複数の脆弱性により、認証された攻撃者がインジェクション攻撃を実行したり、権限を昇格したりす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-privesc-9DVkFpJ8

該当製品

脆弱性のある製品

CVE-2023-20009は、Cisco AsyncOSソフトウェアの脆弱なリリースを実行している場合、仮

想アプライアンスと物理アプライアンスの両方であるCisco ESAおよびCisco Secure Email and Web Managerに影響を与えます。

CVE-2023-20075は、Cisco AsyncOSソフトウェアの脆弱なリリースを実行している場合、仮想アプライアンスと物理アプライアンスの両方のCisco ESAに影響を与えます。

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。

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、これら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-2023-20009がCisco Secure Web Appliance(旧称Cisco Web Security Appliance(WSA))に影響を与えないことを確認しました。

シスコは、CVE-2023-20075がCisco Secure Email & Web ManagerまたはCisco Secure Web Applianceに影響を与えないことを確認しました。

注：シスコポートフォリオの簡素化の一環として、セキュリティ製品の名称を変更し、Cisco Secure というブランド名に統一しています。詳細については、「Cisco Secure が登場」を参照してください。

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-2023-20009:Cisco ESAおよびCisco Secure Email & Web Managerの権限昇格の脆弱性

Cisco ESAおよびCisco Secure Email & Web ManagerのWeb UIおよびCLIの脆弱性により、認証されたリモート攻撃者(Web UI)または認証されたローカル攻撃者(CLI)が権限をルートに昇格できる可能性があります。攻撃者は、オペレータレベル以上の権限を持つ有効なユーザ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、アップロードされたSimple Network Management Protocol(SNMP)コンフィギュレーションファイルの不適切な検証に起因します。攻撃者は、該当デバイスに認証を行い、特別に巧妙に細工されたSNMP設定ファイルをアップロードすることで、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、攻撃者はコマンドをrootとして実行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:CSCwd29901、CSCwd29905
CVE ID：CVE-2023-20009
セキュリティ影響評価（SIR）：高
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-2023-20075:Cisco ESAコマンドインジェクションの脆弱性

Cisco ESAのCLIの脆弱性により、認証されたローカルの攻撃者が該当デバイスで任意のコマンドを実行する可能性があります。

この脆弱性は、CLIでの不適切な入力検証に起因します。攻撃者は、オペレーティングシステムコマンドを正規のコマンドに挿入することで、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、攻撃者は制限付きコマンドプロンプトをエスケープし、CLIプロセスユーザとして基盤となるオペレーティングシステム上で任意のコマンドを実行する可能性があります。この脆弱性を不正利用するには、攻撃者がオペレータレベル以上の権限を持つ有効なユーザ*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。

バグID:CSCwd50043
CVE ID：CVE-2023-20075
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：6.0
CVSSベクトル：CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/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

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お

客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

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。

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。

サービス契約をご利用でないお客様

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 TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）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。

修正済みリリース

次の表に示すように、該当する修正済みの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。

ESA

Cisco AsyncOS ソフトウェアリリース	CVE-2023-20009 の最初の修正済みリリース	CVE-2023-20075 の最初の修正済みリリース
12.5 より前	修正済みリリースに移行。	脆弱性なし

12.5	12.5.3-041	12.5.3-041
13.0	13.0.5-007	13.0.5-007
13.5	13.5.4-038	13.5.4-038
14.0	14.2.1-020	14.2.1-020
14.3	14.3.0-0321	14.3.0-0321

1. このリリースはクラウドベースの製品向けです。

Cisco Secure Email and Web Manager

Cisco AsyncOS ソフトウェアリリース	CVE-2023-20009 の最初の修正済みリリース
12.8 より前	修正済みリリースに移行。
12.8	12.8.1-021
13.8	13.8.1-108
14.0	14.2.0-224
14.31	14.3.0-1201

1. このリリースはクラウドベースの製品向けです。

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 クラウド E メールセキュリティ（CES）には、サービスソリューションの一部として Cisco E メール セキュリティ アプライアンス（ESA）と Cisco Secure Email および 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 CES 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 は、このアドバイザリで説明されているいくつかの脆弱性に対して概念実証段階の

エクスプロイトコードが利用可能であることを認識しています。

Cisco PSIRT では、このアドバイザリに記載されている脆弱性のいかなる悪用も認識していません。

出典

シスコは、CVE-2023-20009およびCVE-2023-20075で説明されている脆弱性を報告していただき、ly1g3に感謝いたします。

また、CVE-2023-20075で説明されている脆弱性を報告していただいたAmlvaro Gutierrez氏に対し、ニーモニックについて謝意を表します。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-privesc-9DVkFpJ8

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	修正済みソフトウェアのリリースに関する情報を更新。	修正済みソフトウェア	Final	2023年2月16日
1.0	初回公開リリース	-	Final	2023年2月15日

利用規約

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。