Cisco E メール セキュリティ アプライアンスと Cisco Secure Email および Web Manager の情報漏えいの脆弱性

High

アドバイザリーID : cisco-sa-esasma-info-dsc-Q9tLuOvM

CVE-2022-20664

初公開日 : 2022-06-15 16:00

バージョン 1.0 : Final

CVSSスコア : 7.7

回避策 : No workarounds available

Cisco バグ ID : CSCvz40090 CSCvz20942

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(旧称Cisco Security Management Appliance(SMA))およびCisco Email Security Appliance(ESA)のWeb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攻撃者が、該当デバイスに接続されたLightweight Directory Access Protocol(LDAP)外部認証サーバから機密情報を取得できる可能性があります。

この脆弱性は、外部認証サーバに対するクエリ中に適切な入力サニタイズが行われないことに起因します。攻撃者は、外部認証Webページを介して巧妙に細工されたクエリを送信することで、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、攻撃者は外部認証サーバからユーザクレデンシャルなどの機密情報にアクセスできる可能性があります。この脆弱性を不正利用するには、攻撃者は有効なオペレータレベル（またはそれ以上）のクレデンシャルを必要とします。

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esasma-info-dsc-Q9tLuOvM

該当製品

脆弱性のある製品

この脆弱性は、次の条件がすべて満たされている場合、Cisco Secure Email and Web Manager(SEM)およびCisco Email Security Appliance(ESA)（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）に影響します。

- 脆弱性のあるCisco AsyncOSソフトウェアリリースを実行している。
- 外部認証を使用するように設定されている。
- 認証プロトコルとしてLDAPを使用している。

注：外部認証がデフォルトで無効になっている。

外部認証が有効になっているかどうかの確認：

1. Cisco Secure Email and Web ManagerまたはCisco ESAのWeb管理インターフェイスにログインします。
2. [System Administration] > [Users] > [External Authentication] > [Enable External Authentication] に移動します。
3. 緑色のチェックマークが表示されている場合は、外部認証が有効になっています。

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、この脆弱性の影響を受けることが分かっています。

シスコでは、この脆弱性が Cisco Secure Web Appliance（旧 Cisco Web セキュリティアプライアンス（WSA））に影響を及ぼさ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

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 Cisco Support and Downloads 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 Cisco Service Contract 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 POS から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

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

この項の該当する表に示すように、適切なリリースにアップグレードすることをお勧めします。次の表では、左列が Cisco AsyncOS ソフトウェアのメジャーリリースを示します。右側の列は、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ているかどうか、およびこの脆弱性に対する修正を含む最初のリリースを示しています。

Cisco Secure Email および Web Manager：CSCvz40090

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)
111 以前	修正済みのリリースに移行。
12	修正済みのリリースに移行。
12.8	修正済みのリリースに移行。
13.0	修正済みのリリースに移行。
13.6	13.6.2-090
13.8	修正済みのリリースに移行。
14.0	修正済みのリリースに移行。
14.1	14.1.0-227

[1] Cisco AsyncOS ソフトウェアのリリース 11 より前については、ソフトウェアメンテナンスが終了しています。この脆弱性の修正を含むサポート対象リリースに移行することをお勧めします。

Cisco E メール セキュリティ アプライアンス： CSCvz20942

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
111 より前のリリース	修正済みのリリースに移行。
11	修正済みのリリースに移行。
12	修正済みのリリースに移行。
13	修正済みのリリースに移行。
14	14.0.1-020

[1] Cisco AsyncOS ソフトウェアのリリース 11 より前については、ソフトウェアメンテナンスが終了しています。この脆弱性の修正を含むサポート対象リリースに移行することをお勧めします。

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。

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。

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esasma-info-dsc-Q9tLuOvM

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	-	最終版	2022 年 6 月 15 日

利用規約