Cisco Secure Email GatewayおよびSecure Email and Web Managerのセキュリティ強化リリース：2026年9月

アドバイザリーID : cisco-sa-hardening-esa-dfCrfXkm
初公開日 : 2026-09-14 16:00
バージョン 1.0 : Final
CVSSスコア : 9.8
回避策 : No workarounds available
Cisco バグ ID :

CVE-2026-76443
CVE-2026-76442
CVE-2026-76441
CVE-2026-76440
CVE-2026-20353

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

プロアクティブなセキュリティと製品の品質に対するシスコの継続的な取り組みの一環として、Cisco Secure Email GatewayおよびCisco Secure Email and Web Managerのエンジニアリングチームは、包括的な社内セキュリティレビューを実施しました。このレビューの結果、社内で発見された複数の脆弱性に対処するソフトウェアのセキュリティ強化リリースが公開されました。

これらの脆弱性は内部テストで発見されました。そのうちの1つが活発に不正利用されることが知られています。詳細については、『Cisco Secure Email Gateway SQLインジェクションの脆弱性』を参照してください。お客様によるパッチ適用を支援し、開示プロセスを効率化するために、シスコはこれらの問題をその根本的な脆弱性クラス（Common Weakness Enumeration（CWE））ごとに分類し、CWE の各グループに 1 つの共通脆弱性識別子（CVE ID）を割り当てました。

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-hardening-esa-dfCrfXkm

該当製品

脆弱性のある製品

これらの脆弱性は、デバイス設定に関係なく、Cisco Secure Email GatewayおよびCisco Secure Email and Web Manager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、これらの脆弱性がCisco Secure Web Applianceには影響を与えないことを確認しました。

詳細

次の表に、これらのソフトウェア強化リリースで対処されている脆弱性クラスの概要を示します。各 CVE ID に割り当てられる CVSS スコアは、その特定の CWE カテゴリ内で最も影響の大きい 1 つの根本的な脆弱性がもたらす可能性がある最大のシビラティ（重大度）を表しています。

CVE ID	CVSS最高スコア	脆弱性クラス（最高レベルのCWE）	説明
CVE-2026-76440	9.8	CWE-23	パストラバーサル（制限されたディレクトリへのパス名の不適切な制限、およびファイルアクセス前の不適切なリンク解決を対象とする）
CVE-2026-76441	9.8	CWE-284	不適切なアクセス制御（承認、認証、権限、およびバイパスなど）
CVE-2026-20353	9.8	CWE-664	リソースのライフタイムを通じた不適切な制御（制御されていないリソース消費、アルゴリズムによる複雑度、再帰/反復、デシリアライゼーション、不適切なリソース初期化を含む）
CVE-2026-76443	9.8	CWE-707	不適切な無害化[1]（コマンド、SQL、コード/評価インジェクション、およびクロスサイトスクリプティングを対象）
CVE-2026-76442	7.5	CWE-1284	入力内の指定数量の検証が不適切（過度な

CVE ID	CVSS最高スコア	脆弱性クラス（最高レベルのCWE）	説明
			リソース消費を引き起こす無制限の数値フィールドをカバー）

1. この脆弱性クラスに属する脆弱性の1つは、アクティブに不正利用されることが確認されています。詳細については、『Cisco Secure Email Gateway SQLインジェクションの脆弱性』を参照してください。

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

これらの脆弱性を修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

修正済みリリース

次の表では、左の列にシスコソフトウェアのリリースを記載しています。右の列は、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るかどうか、およびこれら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。このセクションの表に記載されている適切な修正済み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。

Cisco Secure Email Gatewayリリース	First Fixed Release（修正された最初のリリース）
15.5 以前	15.5.5-014
16.0	修正済みリリースに移行。
16.5	16.5.0-780

Cisco Secure Email and Web Managerリリース	First Fixed Release（修正された最初のリリース）
15.5 以前	15.5.5-006
16.0	修正済みリリースに移行。
16.5	16.5.0-429

ソフトウェアは、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。

CLI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. upgradeを実行します。
2. 「DOWNLOADINSTALL」と入力します。
3. アップグレードするリリースを選択します。
4. アップグレードプロセス全体を通じて適切なオプションを選択します。

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。また、Cisco Secure Email Cloudのサポートに連絡して、ソフトウェアのアップグレードをリクエストすることもできます。

シスコの 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済み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

すでに特記されている場合を除き、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

これらの脆弱性は、既存のテストプロセスおよびフロンティアの AI モデルを使用した内部セキュリティテストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-esa-dfCrfXkm

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	2026年9月14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。