Cisco Secure Email GatewayのSQLインジェクションの脆弱性

アドバイザリーID : cisco-sa-esa-inj-2bLVGmhX
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 : CSCwu56234

CVE-2026-76461

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 Gateway用Cisco AsyncOSソフトウェアの電子メール解析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が基盤となるオペレーティングシステムでルート権限を使用して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、電子メール解析ロジックの不十分な検証に起因します。攻撃者は、悪意のあるSQL文を含む巧妙に細工された電子メールメッセージを該当デバイス経由で送信することで、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、攻撃者は任意のSQL文を実行し、基盤となるオペレーティングシステムでルート権限によるコマンド実行を引き起こす可能性があります。

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。

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-inj-2bLVGmhX

該当製品

脆弱性のある製品

この脆弱性は、デバイスの設定に関係なく、Cisco Secure Email Gatewayの物理および仮想の両方に影響を与えます。

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リストされている製品だけがこの脆弱性の影響を受けることが知られています。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- Cisco Secure Email and Web Manager
- Cisco Secure Web Appliance

セキュリティ侵害の痕跡

この脆弱性の不正利用が試みられたことを確認するには、mail_logsを確認し、疑わしいSQL文を探します。デバイスがクラスタの一部である場合は、各クラスタデバイスのログを確認します。次に、ログで悪意のあるSQL文を検出する方法の例を示します。

```
<#root>

cisco-esa>

grep -i "COPY.*TO PROGRAM" [IronPort Text Mail Logs Log name - Default: mail_logs]
```

出力にエントリが存在する場合は、悪意のあるアクティビティを示している可能性があります。

Cisco Secure Email Cloudでは、CLIにアクセスできない管理者は、記述されているセキュリティ侵害のインジケータを個別にチェックできない場合があります。シスコは、悪意のあるアクティビティが検出されたCisco Secure Email Cloudデバイスを所有するお客様に直接連絡しました。

注：この脆弱性のエクスプロイトに成功すると、脅威アクターはroot権限でコマンドを実行できるようになります。このアクセスレベルにより、悪用の証拠や侵害の痕跡が攻撃者によって削除されたり、隠されたりする可能性があります。シスコでは、管理者が影響を受けるデバイスの外部でネットワークログとファイアウォールログを相互チェックして、疑わしいアクティビティを特定することを強く推奨します。疑わしいアクティビティには、影響を受けるデバイスから外部IPアドレスへの予期しないアップロードや、悪意のあるIPアドレスからのダウンロードなどがあります。

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

シスコでは、回避策や緩和策（該当する場合）は、修正済みソフトウェアリリースへのアップグレードが利用可能になるまでの一時的な解決策であると考えています。この脆弱性を修正し、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 AsyncOS for Cisco Secure Email Gateway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）
15.5 以前	15.5.5-0141
16.0	16.0.4-3021
16.5	16.5.0-780

1. シスコでは、リリース16.5.0-780への移行を強く推奨します。

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。

シスコはすでに、すべてのCisco Secure Email Cloudデバイスをリリース16.5.0-780にアップグレードしています。

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

2026年9月、Cisco PSIRTはこの脆弱性が活発に悪用されていることを認識しました。

出典

この脆弱性は 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-esa-inj-2bLVGmhX

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。