ClamAV OLE2ファイル形式の復号化における Denial of Service(DoS)の脆弱性

Medium

アドバイザリーID : cisco-sa-clamav-ole2-H549rphA
CVE-2025-20128
初公開日 : 2025-01-22 16:00
バージョン 1.0 : Final
CVSSスコア : 5.3
回避策 : No workarounds available
Cisco バグ ID : CSCwm89779 CSCwm89778 CSCwm91582 CSCwm89781

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

ClamAVのObject Linking and Embedding 2(OLE2)復号ルーチンの脆弱性により、認証されていないリモートの攻撃者が該当デバイスにサービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、ヒープバッファオーバーフロー読み取りを可能にする境界チェックの整数アンダーフローに起因します。攻撃者は、該当デバイスの ClamAV によってスキャンされる OLE2 コンテンツを含む細工されたファイルを送信することで、この脆弱性をエクスプロイト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ClamAVスキャンプロセスを終了し、影響を受けるソフトウェアでDoS状態が発生する可能性があります。

この脆弱性の詳細については、ClamAV blogを参照してください。

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-clamav-ole2-H549rphA

該当製品

本アドバイザリの「脆弱性のある製品」セクションには、影響を受ける各製品の Cisco Bug ID が記載されています。Cisco Bug は Cisco Bug Search Tool で検索可能であり、回避策 (使用可能な場合) と修正されたソフトウェア リリースなど、プラットフォーム固有の追加情報が記載され

ます。

脆弱性のある製品

次の表に、本アドバイザリに記載された脆弱性の影響を受けるシスコ製品を示します。詳細については、関連するシスコのバグ ID を参照してください。

影響を受けるシスコ ソフトウェア プラットフォーム	CVSS 基本評価スコア	セキュリティへの影響の評価	Cisco Bug ID	First Fixed Release（修正された最初のリリース）
Linux 向け Cisco Secure Endpoint Connector	6.9	中	CSCwm89778	1.25.1
Cisco Secure Endpoint Connector for Mac	6.9	中	CSCwm89779	1.24.4
Windows 向け Cisco Secure Endpoint Connector	6.9	中	CSCwm89781	7.5.20 8.4.3
セキュアエンドポイントプライベートクラウド	6.9	中	CSCwm91582	4.2.0 と更新されたコネクタ

シスコ製品は、ClamAV の使用環境や用途によって異なる影響を受ける可能性があります。特定のCisco製品に対するこの脆弱性の影響については、このアドバイザリの「詳細情報」の項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。

- Secure Email Gateway
- Cisco Secure Web Appliance

詳細

ClamAV DoS脆弱性の影響を受けるプラットフォーム

セキュリティ影響評価(SIR)が中程度であるこの脆弱性は、Linux、Mac、およびWindowsベースのプラットフォームに影響を与えます。この脆弱性がエクスプロイトされると、スキャンプロセスがクラッシュし、以降のスキャン処理が遅延したり、妨げられたりする可能性があります。ただし、システム全体の安定性には影響しません。脆弱性スコアおよびSIRに関する情報は、Cisco Security Vulnerability Policyの「 セキュリティリスクの評価」セクションを参照してください。

Cisco Secure Endpoint Private Cloudから配布されるCisco Secure Endpoint Connectorは、この脆弱性の影響を受けます。Cisco Secure Endpoint Private Cloudには影響はありません。

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

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完全なアップグレード ソリューション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

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。

左側の列にはシスコソフトウェアリリース、右側の列に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、およびこの脆弱性に対する修正を含むリリースが示されています。

影響を受けるシスコ ソフトウェア プラットフォーム	First Fixed Release（修正された最初のリリース）
Linux 向け Cisco Secure Endpoint Connector	1.25.11
Cisco Secure Endpoint Connector for Mac	1.24.41
Windows 向け Cisco Secure Endpoint Connector	7.5.201 8.4.31
セキュアエンドポイントプライベートクラウド	4.2.0コネクタの更新[2]

1. Cisco Secure Endpoint Connector の更新されたリリースは、Cisco Secure Endpoint ポータルから入手できます。設定されたポリシーに応じて、Cisco Secure Endpoint Connector は自動的に更新されます。
2. Cisco Secure Endpoint Private Cloud用のCisco Secure Endpoint Connectorクライアントの該当リリースが、コネクタリポジトリで更新されています。お客様は、通常のコンテンツ更新プロセスを通じて、これらのコネクタの更新を受けることができます。

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、この脆弱性の報告に関して Google OSS-Fuzz に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-ole2-H549rphA

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	2025年1月22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。