ClamAV の OLE2 ファイル形式解析におけるサービス妨害の脆弱性

High

アドバイザリーID : cisco-sa-clamav-hDffu6t CVE-2024-20290
初公開日 : 2024-02-07 16:00
最終更新日 : 2024-02-13 17:57
バージョン 1.1 : Final
CVSSスコア : 7.5
回避策 : No workarounds available
Cisco バグ ID : CSCwh88484 CSCwh88483

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 OLE2 ファイル形式解析における脆弱性により、認証されていないリモート攻撃者が該当デバイスでサービス妨害（DoS）状態を引き起こす可能性があります。

この脆弱性は、スキャン中の文字列末尾の値に関する誤ったチェックに起因します。これにより、ヒープバッファのオーバーリードが発生する可能性があります。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させることができる可能性があります。その結果、影響を受けるソフトウェアで DoS 状態が発生し、使用可能なシステムリソースが消費されます。

この脆弱性の詳細については、ClamAVブログ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-hDffu6t

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）
Windows 向け Cisco Secure Endpoint Connector	7.5	高	CSCwh88483	7.5.17（2024 年 2 月） 8.2.3.30119
セキュアエンドポイントプライベートクラウド	7.5	高	CSCwh88484	3.8.0 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。特定のシスコ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」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。

- Firepower Threat Defense（FTD）ソフトウェア
- Cisco Secure Email Gateway（旧 Cisco E メール セキュリティ アプライアンス（ESA））
- Linux 向け Cisco Secure Endpoint Connector
- Cisco Secure Endpoint Connector for Mac
- Cisco Secure Web Appliance

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

Windows プラットフォームでの ClamAV DoS 脆弱性の影響

セキュリティ影響評価（SIR）が「高」のこの脆弱性は、Windows ベースのプラットフォームにのみ影響します。これは、Windows ベースのプラットフォームで実行される ClamAV スキャンプロセスが、ループ状態になる可能性のあるサービスであるためです。これにより、使用可能な CPU リソースが消費され、その後のスキャンプロセスで遅延や停止が発生します。脆弱性スコアと SIR については、『Cisco Security Vulnerability Policy』の「Assessing Security Risk」のセク

ションを参照してください。

この脆弱性により、攻撃者が Windows 向け Cisco Secure Endpoint Connector でループ状態を発生させてコネクタの応答を停止し、その結果、DoS 状態が発生する可能性があります。Cisco Secure Endpoint Private Cloud から配布される Windows 向け Cisco Secure Endpoint Connector が、この脆弱性の影響を受けます。

バグ ID：CSCwh88483
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：7.5
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

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

修正済みソフトウェアリリースの詳細については、本アドバイザリの「脆弱性のある製品」セクションに記載されている Cisco Bug ID を参照してください。

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。

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。

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）
Windows 向け Cisco Secure Endpoint Connector	7.5.17（2024 年 2 月）[1] 8.2.3.301191
セキュアエンドポイントプライベートクラウド	3.8.0 と更新されたコネクタ[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 の影響を受ける Cisco Secure Endpoint Connector クライ

アントのリリースは、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 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

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-hDffu6t

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。	「脆弱性のある製品」および「修正済みリリース」	Final	2024 年 2 月 13 日
1.0	初回公開リリース	—	Final	2024 年 2 月 7 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。