シスコ製品に影響するClamAVの脆弱性：2026年11月



Advisory ID : cisco-sa-clamav-multi-e93M3vdA
初公開日 : 2026-11-18 16:00
バージョン 1.0 : Final
CVSSスコア : 7.5
回避策 : No workarounds available
Cisco Bug ID : CSCww14020 CSCww46623 CSCww14023 CSCww14024 CSCwv98582 CSCww34036 CSCwv99250 CSCww14271 CSCww28463 CSCwv96487 CSCwv99257 CSCwv99214 CSCwv99244 CSCww18729

CVE-2026-76411
CVE-2026-76422
CVE-2026-76421
CVE-2026-76430
CVE-2026-76417
CVE-2026-76516
CVE-2026-76416
CVE-2026-76515
CVE-2026-76415
CVE-2026-76414

日本語の情報は原文の英語の非公式な翻訳です。日本語と英語のバージョンに相違がある場合は、英語のバージョンが優先されます。

概要

ClamAVの複数の脆弱性により、リモート攻撃者が設定されたファイルとスキャンの時間制限をバイパスし、サービス妨害(DoS)状態を引き起こし、スキャン操作を中断する可能性があります。

これらの脆弱性の詳細については、本アドバイザリの「詳細情報」セクションを参照してください。

ClamAV のこれら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。

シスコでは、影響を受けるシスコプラットフォームで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ました。これらの脆弱性に対処する回避策はありません。

注記:

- これらの脆弱性のセキュリティ影響評価(SIR)は、Windowsベースのプラットフォームでのみ高くなっています。これらのプラットフォームでは、特権セキュリティコンテキストでClamAVスキャンプロセスが実行されるためです。影響が大きいプラットフォームには、Cisco Secure Endpoint Connector for Windows が含まれます。
- これらの脆弱性の SIR は、Linux および Mac プラットフォームを含む他のプラットフォームでは「中」です。それらのプラットフォームでは、より低い特権のセキュリティコンテキストで ClamAV スキャンプロセスが実行されるためです。影響を受けるプラットフォームには、Linux および Mac 用の Secure Endpoint Connector が含まれます。
- Cisco Secure Endpoint Private Cloud 自体は、これらの脆弱性の影響を受けません。代わりに、Cisco Secure Endpoint Connectorソフトウェアが影響を受けます。

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-multi-e93M3vdA

該当製品

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。

該当するシスコプラットフォーム	CVSS 基本評価スコア	セキュリティへの影響の評価	Cisco Bug ID	第 1 修正済みリリース
Linux 向け Cisco Secure Endpoint Connector	5.3	中間	CSCww14020	1.29.3
Cisco Secure Endpoint Connector for Mac	5.3	中間	CSCww14023	1.27.5
Windows 向け Cisco Secure Endpoint Connector	7.5	高い	CSCww14024	8.6.4
セキュアエンドポイントプライベートクラウド	0.0	是正後は影響なし	CSCww14271	リリース番号未定（2026 年 11 月）

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れら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、これらの脆弱性の影響を受けることが分かっています。

詳細

これらの脆弱性は依存関係にはなく、いずれかの脆弱性をエクスプロイトするために別の脆弱性をエクスプロイトする必要はありません。さらに、いずれかの脆弱性の影響を受けるソフトウェアリリースであっても、他の脆弱性の影響は受けない場合があります。

脆弱性の詳細は以下のとおりです。

CVE-2026-76411:ClamAV Phishcheck機能のDoS脆弱性

ClamAVのフィッシュチェック機能の脆弱性により、認証されていないリモートの攻撃者が該当デバイスにDoS状態を引き起こす可能性があります。

この脆弱性は、URLが処理される際のメモリの不適切な割り当てに起因します。攻撃者は、ソフトウェアによって処理される巧妙に細工されたURLを送信することにより、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 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 状態が発生します。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

バグID: CSCwv98582
CVE ID：CVE-2026-76411
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

CVE-2026-76414:ClamAV Microsoftコンパイル済みHTMLヘルプファイルの無限ループの脆弱性

ClamAVに対するMicrosoftコンパイル済みHTMLヘルプ(CHM)ファイルスキャンの脆弱性により、認証されていないリモートの攻撃者が該当デバイスにDoS状態を引き起こす可能性があります。

この脆弱性は、CHMファイルをスキャンし、内部ファイルポインタを追跡する際の論理エラーが原因です。攻撃者は、巧妙に細工されたCHMファイルをスキャン用に送信することにより、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、無限ループが原因でClamAVデコードプロセスが終了し、影響を受けるソフトウェアでDoS状態が発生する危険性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

バグID: CSCwv99244
CVE ID：CVE-2026-76414
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

CVE-2026-76415:ClamAV YodaのCrypter Portable Executable Unpacker MemoryのRead Underflowの脆弱性

YodaのClamAVのCrypter(yC)Portable Executable(PE)アンパッカー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該当デバイスにDoS状態を引き起こす可能性があります。

この脆弱性は、PEファイルの処理中に負の値をチェックする適切なエラーチェックがないことに起因します。攻撃者は、巧妙に細工されたPEファイルをアンパックするために送信することで、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 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 状態が発生します。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

バグID: CSCwv99214
CVE ID：CVE-2026-76415
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

CVE-2026-76416:ClamAV InstallShieldファイルパーサーの無限ワーカーループの脆弱性

ClamAVのInstallShieldファイルパーサーの脆弱性により、認証されていないリモート攻撃者が該当デバイスにDoS状態を引き起こす可能性があります。

この脆弱性は、InstallShieldファイルパーサーがスキャンを実行する際の不完全なエラーチェックに起因します。攻撃者は、巧妙に細工されたInstallShieldファイルをスキャン対象として送信することで、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、無限のワーカーループが原因でClamAVスキャンプロセスが終了し、影響を受けるソフトウェアでDoS状態が発生する危険性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

バグID: CSCwv99250
CVE ID：CVE-2026-76416
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

CVE-2026-76417:ClamAVオブジェクトのリンクと埋め込みにおけるバージョン2のメモリ枯渇の脆弱性

ClamAVのObject Linking and Embedding version 2(OLE2)ファイルパーサーの脆弱性により、認証されていないリモートの攻撃者が該当デバイスにDoS状態を引き起こす可能性があります。

この脆弱性は、OLE2ファイルパーサーが巧妙に細工されたファイルを解析する際の論理エラーが原因です。攻撃者は、スキャン対象として巧妙に細工されたMicrosoft Compound File Binary(CFB)ファイルを送信することにより、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、攻撃者はすべての使用可能なメモリを割り当てることができ、ClamAVスキャンプロセスが終了し、該当ソフトウェアでDoS状態が発生する可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

バグID: CSCwv99257
CVE ID：CVE-2026-76417
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

CVE-2026-76421:ClamAV LZX CHMファイルデコーダのヒープバッファオーバーフローの脆弱性

ClamAVにおけるCHMファイルスキャン用のLZXデータアルゴリズムの脆弱性により、認証されていないリモートの攻撃者が該当デバイスにDoS状態を引き起こす可能性があります。

この脆弱性は、デコーダ段階でLZXデータアルゴリズムをCHMファイルに適用する際の不適切な境界チェックに起因し、バッファオーバーフローが発生する可能性があります。攻撃者は、巧妙に細工されたCHMファイルをスキャン用に送信することにより、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 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 状態が発生します。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

バグID: CSCww18729
CVE ID：CVE-2026-76421
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

CVE-2026-76422:ClamAVデバッグロギング機能のDoS脆弱性

ClamAVのデバッグロギング機能の脆弱性により、認証されていないリモートの攻撃者が該当デバイスにDoS状態を引き起こす可能性があります。

この脆弱性は、ロギング値の不適切な処理に起因します。攻撃者は、巧妙に細工されたファイルを送信し、デバッグロギングが有効になっているClamAVソフトウェアでスキャンさせることで、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 状態が発生します。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

バグID: CSCwv96487
CVE ID：CVE-2026-76422
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

CVE-2026-76430:eXecutables用ClamAV Ultimate Packerのヒープアウトオブバウンド読み取りの脆弱性

ClamAVのUltimate Packer for eXecutables(UPX)アンパッカー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該当デバイスにDoS状態を引き起こす可能性があります。

この脆弱性は、UPXファイルをアンパックする際の長さチェックが不適切であり、ヒープメモリの範囲外の読み取りが発生する可能性があることに起因します。攻撃者は、巧妙に細工されたUPXファイルをデコード用に送信することで、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ClamAVデコードプロセスを終了させ、影響を受けるソフトウェアでDoS状態を引き起こす可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

バグID: CSCww28463
CVE ID：CVE-2026-76430
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

CVE-2026-76515:ClamAV OLE2スキャン時間バイパスおよびDoS脆弱性

ClamAVのOLE2ファイルパーサーの脆弱性により、認証されていないリモートの攻撃者が設定されたMaxScanTimeを超過し、該当デバイスにDoS状態を引き起こす可能性があります。

この脆弱性は、OLE2ファイルパーサーで巧妙に細工されたファイルを解析する際の非効率性に起因します。攻撃者は、スキャン対象として巧妙に細工されたMicrosoft Compound File Binary(CFB)ファイルを送信することにより、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者はClamAV OLE2パーサーを無限ループに陥れ、結果として該当ソフトウェアでDoS状態が発生する可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

バグID: CSCww46623
CVE ID：CVE-2026-76515
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

CVE-2026-76516:ClamAV eXtensible ARchive GZIPファイルサイズのバイパスおよびDoSの脆弱性

ClamAVのeXtensible ARchive(XAR)GZIPファイルパーサー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、設定されているMaxFileSizeを超過し、該当デバイスにDoS状態を引き起こす可能性があります。

この脆弱性は、XAR GZIPファイルパーサーを使用して特定の形式のファイルを解析する際の非効率性に起因します。攻撃者は、巧妙に細工されたXAR GZIPファイルをスキャン対象として送信することで、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者はClamAVをMaxFileSizeを超え、無限ループに陥る可能性があり、DoS状態を引き起こします。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

バグID: CSCww34036
CVE ID：CVE-2026-76516
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

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。

シスコ製品	Cisco Bug ID	第 1 修正済みリリース
Linux用セキュアエンドポイントコネクタ[1]	CSCww14020	1.29.3
Secure Endpoint Connector for Mac[1]（ベータ版）	CSCww14023	1.27.5
Windows[1]用セキュアエンドポイントコネクタ	CSCww14024	8.6.4
セキュアエンドポイントプライベートクラウド[2]	CSCww14271	リリース番号未定（2026 年 11 月）

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。設定したポリシーに応じて、Cisco Secure Endpoint Connectorが自動的に更新されることがあります。
2. Cisco Secure Endpoint Connector の影響を受けるリリースは、クライアントリリースが入手可能になった後、Cisco Secure Endpoint Private Cloud のコネクタリポジトリで更新されます。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。

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

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。

送信元

CVE-2026-76414、CVE-2026-76415、CVE-2026-76416、およびCVE-2026-76417：これらの脆弱性を報告していただいたNebula Security社に感謝いたします。

CVE-2026-76411、CVE-2026-76421、およびCVE-2026-76422：シスコは、これらの脆弱性を報

告していただいたThreatBookのFeng Xue氏とXGPT氏に感謝いたします。

CVE-2026-76430：この脆弱性を報告していただいたThreatBookのFeng Xue氏とXGPT氏、およびNicola Ruaro氏に感謝いたします。

CVE-2026-76515：シスコは、この脆弱性を報告していただいたシドニー大学のDisproof AI Lab（Liyi Zhou、Ziyue Wang、Strick、Maurice、およびChenchen Yu）のセキュリティ調査チームに感謝いたします。

CVE-2026-76516：この脆弱性を報告していただいた独立したセキュリティ研究者Paramut Suwannabut氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-multi-e93M3vdA

改訂履歴

バージョン	説明	セクション	Status	日付
1.0	初版リリース	—	Final	2026年11月18日

利用規約

ソフトウェアのダウンロードおよびテクニカルサポート

Cisco.com の シスコサポート & ダウンロードページには、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。お客様がソフトウェアをダウンロードできるのは、シスコから直接、あるいはシスコ認定再販業者やシスコ認定パートナーを通じて調達されたもので、ライセンスが有効なものに限ります。

シスコから直接購入したがシスコのサービス契約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購入先から入手できない場合は、Cisco Technical Assistance Center（TAC）に連絡してアップグレードを入手してください。 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。

ソフトウェアのアップグレードを検討する際には、関連す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。

利用規約の詳細

シスコは、商品適格性または特定目的への適合性に関する保証を含め、明示的か黙示的かを問わず、いかなる種類の保証も表明しません。前述の一般論に限定されることなく、シスコは、本情報の正確性または完全性を保証するものではありません。コンテンツは「現状のまま」提供されます。本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。

本セキュリティアドバイザリに含まれる情報のコピーや要約には、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。本セキュリティアドバイザリの最新版については、シスコ セキュリティ アドバイザリ ページをご覧ください。Cisco 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評価します。詳細については、シスコのセキュリティ脆弱性ポリシーを参照してください。

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。