シスコ製品に影響を与えるClamAV脆弱性：2026年8月

High

アドバイザリーID : cisco-sa-clamav-WuuvVd26
初公開日 : 2026-08-07 16:00
バージョン 1.0 : Interim
CVSSスコア : 7.5
回避策 : No workarounds available
Cisco バグ ID : CSCwu65985 CSCwu99410 CSCwu59475 CSCwu78432 CSCwu34288 CSCwv57797

CVE-2026-20338
CVE-2026-20339
CVE-2026-20347
CVE-2026-20337
CVE-2026-20348
CVE-2026-20345
CVE-2026-20346

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 における複数の脆弱性により、リモートの攻撃者がサービス妨害（DoS）状態を引き起こし、スキャン動作を中断させ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、該当す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する予定です。これらの脆弱性に対処する回避策はありません。

注：

- 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についてのみ「高」です。これは、そ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。ただし、そのデバイスから配布される Cisco Secure Endpoint Connector ソフトウェアは影響を受けます。

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-WuuvVd26

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。

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	5.3	中間	CSCwv87285	リリース番号未定（2026年8月）
Cisco Secure Endpoint Connector for Mac	5.3	中間	CSCwv87286	リリース番号未定（2026年8月）
Windows 向け Cisco Secure Endpoint Connector	7.5	高	CSCwv87283	リリース番号未定（2026年8月）

Secure Endpoint Private Cloudは、これらの脆弱性の影響を受けません。ただし、修正済みソフトウェアをクラウドからエンドポイントにプッシュする必要があります。Secure Endpoint Private Cloudリリース4.2.8以降には、エンドポイント用の修正済みソフトウェアが含まれています。詳細は、Cisco Bug ID CSCwv91588を参照してください。

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-2026-20337:ClamAV Zipファイル形式の範囲外の書き込み処理の脆弱性

ClamAVのzipアーカイブ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、スキャン時にzipファイルのコンテンツの境界チェックが不適切であり、境界外の書き込み状態が発生する可能性があることに起因します。攻撃者は、巧妙に細工したzipファイルをスキャンの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。

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。

バグID: CSCwu34288
CVE ID：CVE-2026-20337
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-2026-20338:ClamAV Zipファイル形式処理のメモリ破損の脆弱性

ClamAVのzipアーカイブ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、スキャン中にzipファイルのコンテンツを処理する際のメモリ処理が不適切なことに起因します。攻撃者は、巧妙に細工したzipファイルをスキャンの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、攻撃者はメモリの二重解放の結果としてClamAVスキャンプロセスを終了させ、結果として該当ソフトウェアでDoS状態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。

バグID: CSCwv57797
CVE ID：CVE-2026-20338
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-2026-20339:ClamAV PESpinファイル形式処理における整数オーバーフローの脆弱性

ClamAVのPESpinファイル形式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、該当デバイスのメモリ破損の結果としてDoS状態を引き起こしたり、その他の影響を受ける可能性があります。

この脆弱性は、スキャン時のPESpinファイルのコンテンツに対する不適切な境界チェックに起因し、整数オーバーフロー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 PESpin コンテンツを含む巧妙に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。

バグID: CSCwu78432
CVE ID：CVE-2026-20339
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-2026-20345:ClamAV GPTファイルフォーマット処理におけるメモリ破損の脆弱性

ClamAVのGPTファイル形式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、該当デバイスのメモリ破損の結果としてDoS状態を引き起こしたり、その他の影響を受ける可能性があります。

この脆弱性は、endian変換操作の不適切な処理に起因します。この処理により、範囲外のバッファ書き込み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GPTファイルを送信して該当デバイスでClamAVによるスキャンを受けることで、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。

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。

バグID: CSCwu59475

CVE ID：CVE-2026-20345
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-2026-20346:ClamAV PDFファイルフォーマット処理のメモリ破損の脆弱性

ClamAVのPDFファイル形式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、該当デバイスのメモリ破損の結果としてDoS状態を引き起こしたり、その他の影響を受ける可能性があります。

この脆弱性は、スキャン時にPDFファイルのコンテンツの境界チェックが不適切であり、範囲外のバッファ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PDFファイルを送信して該当デバイスでClamAVによるスキャンを受けることで、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。

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。

バグID: CSCwu65985
CVE ID：CVE-2026-20346
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-2026-20347:ClamAV Mach-Oファイルフォーマット処理のメモリ破損の脆弱性

ClamAVのMach-Oファイル形式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、該当デバイスのメモリ破損の結果として、DoS状態を引き起こしたり、その他の影響を受ける可能性があります。

この脆弱性は、スキャン時にマッハ－Oファイル内のコンテンツの境界チェックが不適切であり、範囲外のバッファ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Mach-Oファイルを送信して該当デバイスでClamAVによるスキャンを受けることで、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。

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。

バグID: CSCwu65985

CVE ID：CVE-2026-20347
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-2026-20348:ClamAV XARファイルフォーマット処理のメモリ破損の脆弱性

ClamAVのXARファイル形式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、該当デバイスのメモリ破損の結果としてDoS状態を引き起こしたり、その他の影響を受ける可能性があります。

この脆弱性は、スキャン中のXARファイルのコンテンツに対する不適切な境界チェックに起因します。攻撃者は、ClamAVによってスキャンされるXARコンテンツを含む巧妙に細工されたファイルを該当デバイスに送信することで、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。

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。

バグID: CSCwu99410
CVE ID：CVE-2026-20348
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。これらの脆弱性を完全に修正し、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	First Fixed Release（修正された最初のリリース）
Linux 向け Cisco Secure Endpoint Connector	CSCwv87285	リリース番号未定（2026年8月）[1]
Cisco Secure Endpoint Connector for Mac	CSCwv87286	リリース番号未定（2026年8月）[1]
Windows 向け Cisco Secure Endpoint Connector	CSCwv87283	リリース番号未定（2026年8月）[1]
セキュアエンドポイントプライベートクラウド	CSCwv91588	4.2.8 以降[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。

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は、CVE-2026-20337およびCVE-2026-20338で説明されている脆弱性に概念実証エクスプロイトコードが利用できることを認識しています。

Cisco PSIRTでは、本アドバイザリに記載されているその他の脆弱性のプルーフオブコンセプトエクスプロイトコードを確認していません。

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、これらの脆弱性を報告していただいた次の研究者に感謝いたします。

- Atuin:Tencent Xuanwu LabのTianchu Chen氏による自動脆弱性検出エンジン：CVE-2026-20345
- Daggolu Rakesh:CVE-2026-20338
- Feng Xue: CVE-2026-20339
- GitHubのKevin Stubbings氏：CVE-2026-20337
- leduckhuong：CVE-2026-20348

- Talence SecurityのTristan Madani氏：CVE-2026-20346およびCVE-2026-20347
- Yazdan Soltani:CVE-2026-20338およびCVE-2026-20339

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-WuuvVd26

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	—	Interim	2026年8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。