シスコ製品に影響を与えるClamAV脆弱性：2026年7月

アドバイザリーID : cisco-sa-clamav-88cFYyxR
初公開日 : 2026-07-01 16:00
最終更新日 : 2026-07-02 20:52
バージョン 1.1 : Final
CVSSスコア : 7.5
回避策 : No workarounds available
Cisco バグ ID : CSCwt57454 CSCwt62779 CSCwu22472 CSCwt62774 CSCwt62781 CSCwt44538 CSCwu18798

CVE-2026-20217
CVE-2026-20215
CVE-2026-20216
CVE-2026-20213
CVE-2026-20214
CVE-2026-20244
CVE-2026-20243

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の複数の脆弱性により、リモート攻撃者がサービス拒否(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のこれらの脆弱性についての詳細は、ClamAVブログを参照してください。

シスコは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ています。これらの脆弱性に対処する回避策はありません。

注：

- Windowsベース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、これらの脆弱性のSecurity Impact Rating(SIR)は「高」です。影響の大きいプラットフォームには、Cisco Secure Endpoint Connector for Windowsなどがあります。
- これらの脆弱性に対するSIRは、LinuxやMacプラットフォームなどの他のプラットフォーム

ではMediumです。これらのプラットフォームでは、権限の低い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。該当するプラットフォームには、LinuxおよびMac用のセキュアエンドポイントコネクタが含まれます。
- 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、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-88cFYyxR

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	CSCwt81503	1.29.0
Cisco Secure Endpoint Connector for Mac	5.3	中間	CSCwt81504	1.27.2
Windows 向け Cisco Secure Endpoint Connector	7.5	高	CSCwt81501	8.6.2
セキュアエンドポイントプライベートクラウド	0.0	影響なし	CSCwu55927	4.2.8 以降

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製品に対するこれらの脆弱性の影響についての詳細は、このアドバイザリの「詳細情報」セクションを参照してください。

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。

シスコは、これらの脆弱性が次のシスコ製品に影響を与えないことを確認しました。

- Secure Email Gateway
- セキュアWebゲートウェイ

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-2026-20216:ClamAV InstallShieldファイル解析のDoS脆弱性

ClamAVのInstallShieldファイル形式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、ファイルスキャン中の一時リソース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InstallShield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し、一時的に使用可能なシステムリソースを消費し、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。

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。

CVE ID：CVE-2026-20216
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

ClamAVメモリ破損の脆弱性

ClamAVにSIRが存在する次の脆弱性は、ClamAVを使用する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。

攻撃者が、Cisco Secure Endpoint Connector for Windowsを使用する該当デバイスに対してこのクラスの脆弱性を不正利用すると、スキャンエンジンのプロセスが終了し、エンドポイントが応答しなくなり、回復するためにシステムのリブートなどの手動操作が必要になる可能性があるため、DoS状態が発生する可能性があります。

Windowsベースのプラットフォームでは、攻撃者は同様の脆弱性を使用してリモートコード実行を実現しています。ただし、このアドバイザリに記載されている脆弱性に対するリモートコード実行の可能性を示す証拠は存在しません。ほとんどの状況では、プラットフォームとメモリの保護により、特に最新の64ビットアーキテクチャを備えたシステムにおいて、コード実行に対する

これらの脆弱性の実用的な不正利用が防止されます。レガシーの32ビットWindowsプラットフォームを実行しているシステムでは、悪用が成功するリスクが高くなります。

Cisco Secure Endpoint Connector for Linux and Macでは、SIRはMediumです。これらの脆弱性がエクスプロイトされると、スキャンエンジンのプロセスが終了したり、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。

脆弱性のスコアおよびSIRの詳細については、Cisco Security Vulnerability PolicyのSecurity Risk Assessment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、これらの脆弱性の影響を受けます。Cisco Secure Endpoint Private Cloud自体には影響しません。

CVE-2026-20213:ClamAV PEファイルフォーマット処理のメモリ破損の脆弱性

ClamAVのPEファイル形式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DoS状態を引き起こしたり、影響を受けるデバイスのメモリ破損に起因するその他の拡張された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PEファイルのコンテンツの境界チェックが不適切であり、範囲外のバッファ書き込みが発生する可能性があることに起因します。攻撃者は、該当デバイスでClamAVによってスキャンされるPE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、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。

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。

CVE ID：CVE-2026-20213
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-2026-20214:ClamAV FSG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FSGファイル形式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DoS状態を引き起こしたり、影響を受けるデバイスのメモリ破損に起因する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FSGファイルのコンテンツの境界チェックが不適切であり、範囲外のバッファ書き込みが発生する可能性があることに起因します。攻撃者は、FSGで圧縮され、ClamAVによってスキャンされるポータブル実行可能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、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。

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。

CVE ID：CVE-2026-20214
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-2026-20215:ClamAV 7zファイルフォーマット処理のメモリ破損の脆弱性

ClamAVの7zファイル形式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DoS状態を引き起こしたり、影響を受けるデバイスのメモリ破損に起因する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7zファイルのコンテンツの境界チェックが不適切であり、範囲外のバッファ書き込みが発生する可能性があることに起因します。攻撃者は、該当デバイスでClamAVによってスキャンされる7z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、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。

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。

CVE ID：CVE-2026-20215
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-2026-20217:ClamAV PESpin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DoS状態を引き起こしたり、影響を受けるデバイスのメモリ破損に起因するその他の拡張された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ます。この結果、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、該当デバイスで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、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。

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。

CVE ID：CVE-2026-20217
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-2026-20243:ClamAV ALZ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ALZファイル形式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DoS状態を引き起こしたり、影響を受けるデバイスのメモリ破損に起因するその他の拡張された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ALZファイルのコンテンツの境界チェックが不適切であり、範囲外のバッファ書き込みが発生する可能性があることに起因します。攻撃者は、ClamAVによってスキャンされるALZ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、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。

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。

CVE ID：CVE-2026-20243
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-2026-20244:ClamAV DMGファイルフォーマット処理のメモリ破損の脆弱性

ClamAVのDMGファイル形式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DoS状態を引き起こしたり、影響を受けるデバイスのメモリ破損に起因するその他の拡大された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DMGファイルのコンテンツの境界チェックが不適切なことに起因します。この結果、32ビットプラットフォームでのみ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、該当デバイスでClamAVによってスキャンされるDMG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、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。

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。

CVE ID：CVE-2026-20244
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	Fixed Release Availability
Linux 向け Cisco Secure Endpoint Connector	CSCwt81503	1.29.01
Cisco Secure Endpoint Connector for Mac	CSCwt81504	1.27.21
Windows 向け Cisco Secure Endpoint Connector	CSCwt81501	8.6.21
セキュアエンドポイントプライベートクラウド	CSCwu55927	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。

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。

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方々に感謝いたします。

- CVE-2026-20213、CVE-2026-20214、およびCVE-2026-20215によるTrail of BitsのDavid Pokora氏
- Calif.ioとクロードおよびアントロピック研究の協力：CVE-2026-20213
- Atuin:Automated Vulnerability Discovery Engine、Tencent Xuanwu LabのTianchu Chen氏：CVE-2026-20213、CVE-2026-20214、CVE-2026-20217
- Niv MosheとTrendAI Zero Day Initiative:CVE-2026-20215

- 水： CVE-2026-20216

- ヤズダン・ソルターニー氏：CVE-2026-20243
- getresponseセキュリティチームのpawlokおよびbarteq:CVE-2026-20243
- leduckhuong:CVE-2026-20243

- スタンレー・ジョン・トビアス氏：CVE-2026-20244

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-88cFYyxR

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	研究者クレジットを追加。	脆弱性のソース	Final	2026年7月2日
1.0	初回公開リリース	—	Final	2026年7月1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。