ClamAVカスケードスタイルシートのイメージ解析エラー処理におけるDoS脆弱性

Medium

アドバイザリーID : cisco-sa-clamav-css-Fn4QSZ
初公開日 : 2026-03-04 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 : CSCwr70255 CSCwr70252 CSCwr70257 CSCwr70268

CVE-2026-20031

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HTMLカスケードスタイルシート(CSS)モジュールの脆弱性により、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、UTF-8文字列を分割する際の不適切なエラー処理に起因します。攻撃者は、巧妙に細工されたHTML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、攻撃者はスキャンプロセスを終了でき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。

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-css-Fn4QSZ

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	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	中間	CSCwr70252	1.28.1
Cisco Secure Endpoint Connector for Mac	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	中間	CSCwr70255	1.27.2
Windows 向け Cisco Secure Endpoint Connector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	中間	CSCwr70268	8.6.0
セキュアエンドポイントプライベートクラウド	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	中間	CSCwr70257	コネクタが更新された 4.2.7以前

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
- 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アセスメント」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

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

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。

左の列にはシスコのプラットフォームが、右の列にはこの脆弱性に対する修正が含まれた最初のソフトウェアリリースが記載されています。

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	1.28.11
Cisco Secure Endpoint Connector for Mac	1.27.21
Windows 向け Cisco Secure Endpoint Connector	8.6.01
セキュアエンドポイントプライベートクラウド	コネクタが更新された4.2.7以前[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やその公表は確認しておりません。

出典

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-css-Fn4QSZ

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	2026年3月4日

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 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。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、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。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

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。