

シスコ製品に影響するClamAV DMGファイル解析XMLエンティティ拡張の脆弱性：2023年2月

Medium アドバイザリーID : cisco-sa-clamav-xxe-TcSZduhN [CVE-2023-20052](#)
初公開日 : 2023-02-15 16:00
最終更新日 : 2023-02-15 20:15
バージョン 1.1 : Final
CVSSスコア : [5.3](#)
回避策 : No workarounds available
Cisco バグ ID : [CSCwd87111](#)
[CSCwd87112](#) [CSCwd87113](#)

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

2023年2月15日に、ClamAVスキャンライブラリの次の脆弱性が公開されました。

ClamAVバージョン1.0.0以前、0.105.1以前、および0.103.7以前のDMG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の機密情報にアクセスする可能性があります。

この脆弱性は、XMLエンティティ置換を有効にすることによってXML外部エンティティインジェクション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DMG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スキャンプロセスによって読み取られる可能性のあるファイルからバイトをリークする可能性があります。

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。

このアドバイザリーは、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-xxe-TcSZduhN>

該当製品

シスコは製品ラインを調査して、この脆弱性により影響を受ける可能性がある製品を特定しまし

た。

「脆弱性が存在する製品」の項には、影響を受ける製品の Cisco Bug ID を示します。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。

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ない製品は、脆弱性が存在しないと判断されています。

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。将来のソフトウェアリリース日が示されている場合、その日付はこのアドバイザリの上部にある最終更新日時点でシスコが把握しているすべての情報に基づいた日付になります。このソフトウェアリリースの日付は、試験結果や優先される機能や修正の提供等いくつかの理由により変更される場合があります。

シスコ製品	Cisco Bug ID	Fixed Release Availability
Secure Endpoint(以前のAdvanced Malware Protection(AMP)for Endpoints、Linux用)	CSCwd87111	1.20.21
Secure Endpoint(旧称Advanced Malware Protection(AMP) for Endpoints、MacOS)	CSCwd87112	1.21.11
Secure Endpoint(旧称Advanced Malware Protection(AMP) for Endpoints、Windows用)	CSCwd87113	7.5.91 8.1.5
セキュアエンドポイントプライベートクラウド	CSCwe18204	3.6.0以降に更新されたコネクタ ²

1. Cisco Secure Endpointの更新リリースは、[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は自動的に更新されます。
2. Cisco Secure Endpoint Private Cloud用のCisco Secure Endpointクライアントの該当リリースが、connectorsリポジトリで更新されました。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取ります。

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。

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。

- セキュアEメールゲートウェイ（旧称：Eメールセキュリティアプライアンス）

- Cisco Secure Email および Web Manager (旧セキュリティ管理アプライアンス)
- セキュアWebアプライアンス (旧称: Webセキュリティアプライアンス)

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。

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) 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を確認していません。

出典

シスコは、この脆弱性を報告していただいたSimon Scannell氏に感謝いたします。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-xxe-TcSZduhN>

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	ClamAV開示日を2月15日に変更しました。	要約	Final	2023年2月15日
1.0	初回公開リリース	-	Final	2023年2月15日

利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザーの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、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。