ClamAV HFS+パーティションスキャンバッファオーバーフローの脆弱性がシスコ製品に影響を与える：2023年2月

Critical

アドバイザリーID : cisco-sa-clamav-q8DThCy

CVE-2023-20032

初公開日 : 2023-02-15 16:00

最終更新日 : 2023-02-22 14:09

バージョン 1.4 : Final

CVSSスコア : 9.8

回避策 : No workarounds available

Cisco バグ ID : CSCwd74132 CSCwd74133 CSCwd74134 CSCwd74135 CSCwe18204

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、ClamAVスキャニングライブラリに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HFS+パーティション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任意のコードを実行する可能性があります。

この脆弱性は、ヒープバッファオーバーフローの書き込みを引き起こす可能性のあるバッファサイズチェックが欠落していることに起因します。攻撃者は、該当デバイスのClamAVによってスキャンされる巧妙に細工されたHFS+パーティション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スキャニングプロセスの権限で任意のコードを実行するか、またはプロセスをクラッシュさせ、サービス拒否(DoS)状態を引き起こす可能性があります。

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。

注：

- この脆弱性に対する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重要です。これらのプラットフォームでは、特権を持つ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。重大な影響を受けるプラットフォームには、Cisco Secure Endpoint Connector for Windowsが含まれます。
- この脆弱性に対する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Mediumです。これらのプラットフォームでは、より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。影響を受けるプラットフォームには、Cisco Secure Web Appliance、Secure Endpoint Connector for Linux and Macなどがあります。
- Cisco Secure Endpoint Private Cloud自体は、こ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-q8DThCy

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(旧称Advanced Malware Protection(AMP) for Endpoints、Linux)	CSCwd74133	1.20.21
Secure Endpoint(旧称Advanced Malware Protection(AMP) for Endpoints、MacOS)	CSCwd74134	1.21.11
Secure Endpoint(旧称Advanced Malware Protection(AMP) for Endpoints、for Windows)	CSCwd74135	7.5.91 8.1.5
セキュアエンドポイントプライベート	CSCwe182	

クラウド	04	コネクタが更新された3.6.0以降[2]
Secure Web Appliance（旧称Web Security Appliance）	CSCwd74132	12.5.6 (May 2023) 14.0.4-005 14.5.1-013（2023 年 3 月） 15.0.0-254 (April 2023)

1. Cisco Secure Endpointの最新リリースは、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が自動的に更新されます。
2. Cisco Secure Endpoint Private Cloudに関するCisco Secure Endpoint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ることができます。

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。

- Secure 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）

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、この脆弱性によってバッファオー

バーフローとその後のプロセス終了が引き起こされる可能性があることを示す、コンセプト実証が利用可能であることを認識しています。

この脆弱性を詳しく説明している追加の技術情報も利用できます。

このアドバイザリで説明されている脆弱性の悪用に関する情報は Cisco PSIRT に寄せられていません。

出典

シスコは、この脆弱性を報告していただいたサイモン・スキャネルに感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-q8DThCy

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.4	コンセプト実証情報を更新。	不正利用事例と公式発表	Final	2023 年 2 月 22 日
1.3	プラットフォームに基づく脆弱性の影響を明確化。ClamAV ブログへのリンクを更新。	要約	Final	2023 年 2 月 21 日
1.2	Secure Web Appliance の 2 つの修正リリースおよび提供開始日を追加。	脆弱性が存在する製品	Final	2023年2月17日
1.1	ClamAV公開日を2月15日に変更。	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

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。