Cisco AMP for EndpointsのMacコネクタソフトウェアのファイルスキャンにおけるDoS脆弱性

Medium

アドバイザリーID : cisco-sa-amp4emac-dos-kfKjUGtM
初公開日 : 2020-05-20 16:00
バージョン 1.0 : Final
CVSSスコア : 6.1
回避策 : No workarounds available
Cisco バグ ID : CSCvt61369

CVE-2020-3314

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

Cisco AMP for Endpoints Mac Connectorソフトウェアのファイルスキャンプロセスの脆弱性により、ローカルファイルのスキャン中にスキャンエンジンがクラッシュし、AMPコネクタが再起動してCisco AMP for Endpointsサービスのサービス妨害(DoS)状態が発生する可能性があります。

この脆弱性は、特定のファイル属性の不十分な入力検証に起因します。攻撃者は、該当システムのユーザに巧妙に細工されたファイルを提供することにより、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Cisco AMP for Endpointsサービスをクラッシュさせ、悪意のある可能性のあるファイルの検出とロギングを逃す可能性があります。ファイルのスキャンを続行すると、Cisco AMP for EndpointsサービスがDoS状態にな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-amp4emac-dos-kfKjUGtM

該当製品

脆弱性のある製品

公開時点では、この脆弱性はリリース1.12.3.738より前のCisco AMP for Endpoints Mac Connectorソフトウェアリリースに影響を与えました。

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。

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。

- AMP for Endpoints Windows Connectorソフトウェア
- エンドポイント向けAMP Linuxコネクタソフトウェア
- エンドポイント向けAMP Androidコネクタソフトウェア

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

ソフトウェアのアップグレードを検討する際には、[シスコのセキュリティアドバイザリおよびアラート（Cisco Security Advisories and Alerts）] 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完全なアップグレード ソリューション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。

修正済みリリース

公開時点では、Cisco AMP for Endpoints Mac Connectorソフトウェアリリース1.12.3.738以降にこの脆弱性に対する修正が含まれています。

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。

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

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-amp4emac-dos-kfKjUGtM

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	2020 年 5 月 20 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。