

# Cisco AMP for Endpoints LinuxコネクタおよびAMP for Endpoints Macコネクタソフトウェアのメモリバッファの脆弱性



アドバイザリーID : cisco-sa-amp4elinux-h33dkrvb [CVE-2020-3343](#)

初公開日 : 2020-05-20 16:00 [CVE-2020-](#)

バージョン 1.0 : Final [3344](#)

CVSSスコア : [5.5](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCvt72806](#) [CSCvt72810](#)

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

LinuxコネクタソフトウェアのCisco AMP for EndpointsとMacコネクタソフトウェアのCisco AMP for Endpointsの脆弱性により、認証されたローカル攻撃者が該当デバイスでバッファオーバーフローを引き起こす可能性があります。

この脆弱性は、入力に対する不十分な検証に起因します。攻撃者は、巧妙に細工されたパケットを該当デバイスに送信することにより、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て再起動させ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-amp4elinux-h33dkrvb>

## 該当製品

### 脆弱性のある製品

この脆弱性の公開時点では、次のシスコ製品に影響を与えていました。

- リリース1.12.3.698より前のエンドポイント用AMP Linuxコネクタソフトウェアリリース

- リリース1.12.3.738より前のエンドポイント用AMP Macコネクタソフトウェアリリース

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Cisco AMP for Endpoints Windows ConnectorソフトウェアおよびCisco AMP for Endpoints Android Connectorソフトウェアには影響を与えないことを確認しました。

## 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、次のシスコ製品にこの脆弱性に対する修正が含まれています。

- AMP for Endpoints Linux Connectorソフトウェアリリース1.12.3.698以降
- AMP for Endpoints Mac Connectorソフトウェアリリース1.12.3.738以降

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-amp4elinux-h33dkrvb>

## 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

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。