脆弱性を前もって積む Windows DLL の Cisco Advanced Malware Protection for Endpoints

Medium	**アドバイザリーID :** cisco-sa-20181029-amp-dll **初公開日 :** 2018-10-29 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 6.7 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvm93525	CVE-2018-15452

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

Windows のエンドポイントのための Cisco Advanced Malware Protection （ AMP ）の DLL ロードコンポーネントの脆弱性はサービスをスキャンするシステムを無効に するか、または無許可侵入の検出を防ぐ他の処置をとる認証された、ローカル攻撃者を可能にする可能性があります。 この脆弱性を不正利用するために、攻撃者は Windows システムの管理資格情報がある必要があります。

脆弱性はランタイムにシステム プロセスによってロードされるリソースの不適当な有効性確認が原因です。 攻撃者は悪意のある DLL ファイルを細工 し、ターゲットのシステムに特定の場所に置くことによってこの脆弱性を不正利用する可能性があります。 正常なエクスプロイトは攻撃者がターゲットのシステムのスキャン サービスを無効に し、最終的にシステムがそれ以上の不正侵入から保護されることを防ぐことを可能にする可能性があります。

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181029-amp-dll

該当製品

脆弱性のある製品

この脆弱性は Cisco AMP for Endpoints に影響を与えます。 該当するソフトウェア リリースについての情報に関しては、このアドバイザリの上で Cisco バグ ID を参照して下さい。

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 脆弱性が存在する製品のセクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

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、本アドバイザリ上部の Cisco Bug ID を参照ください。

ソフトウェアのアップグレードを検討する際には、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。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例は確認していません。

出典

この脆弱性は、Cisco TAC のサポート ケースの解決中に発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181029-amp-dll

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2018-October-29

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。