Cisco Advanced Malware Protection for Endpoints on Windows DLLのプリロードに関する脆弱性

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のエンドポイント向けCisco Advanced Malware Protection(AMP)のDLLロードコンポーネントの脆弱性により、認証されたローカルの攻撃者がシステムスキャンサービスを無効にしたり、他のアクションを実行して不正な侵入の検出を防止したりする可能性があります。この脆弱性を不正利用するには、攻撃者はWindowsシステムで管理者クレデンシャルを持っている必要があります。

この脆弱性は、実行時にシステムプロセスによってロードされるリソースの検証が不適切であることに起因します。攻撃者は、悪意のある DLL ファイルを細工し、それをターゲット システム上の特定の場所に配置することで、この脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功すると、攻撃者はターゲットシステムのスキャンサービスを無効にし、最終的にシステムをそれ以上の侵入から保護できなくなります。

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://sec.cloudapps.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に影響します。該当するソフトウェアリリースの詳細

については、このアドバイザリの冒頭にあるCisco Bug ID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。

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、[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。

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不正利用事例とその公表は確認しておりません。

出典

この脆弱性は Cisco TAC サポートケースの解決中に発見されました。

URL

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

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	2018年10月29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。

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。