脆弱性を前もって積む Cisco Immunet Antimalware インストーラ DLL

Medium	**アドバイザリーID :** cisco-sa-20171115-iami **初公開日 :** 2017-11-15 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 4.2 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvf23928	CVE-2017-12312

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 Immunet antimalware インストーラの信頼できないサーチ パス脆弱性は管理権限のローカルユーザが巧妙に細工された DLL が攻撃者によって置かれた現在の作業ディレクトリのインストーラを実行する場合 DLL ハイジャックによって任意 の コードを実行する認証された、ローカル攻撃者を可能にする可能性があります。

脆弱性はロードされる前にパスの不完全な入力の検証および DLL ファイルのファイル名が原因です。 攻撃者は悪意のある DLL ファイルを作成し、特定のシステム 登録簿にそれをインストールする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システム アカウントと同等の特権の根本的な Microsoft ウィンドウ ホストのコマンドを実行することを可能にする可能性があります。 攻撃者は有効 な ユーザ 資格情報がこの脆弱性を不正利用することを必要とします。

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。
115-iami

該当製品

脆弱性のある製品

この脆弱性は Cisco Immunet Antimalware インストーラに影響を与えます。 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

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

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。

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やその公表を確認していません。

出典

この脆弱性は Fortinet の FortiGuard ラボの Kushal Arvind Shah によって Cisco に報告されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171115-iami

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2017-November-15

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。