

Cisco AnyConnect Client for Windowsの権限昇格の脆弱性



アドバイザリーID : Cisco-SA-20150623-[CVE-2015-4211](#)
CVE-2015-4211
初公開日 : 2015-06-23 17:53
バージョン 1.0 : Final
CVSSスコア : [6.8](#)
回避策 : No Workarounds available
Cisco バグ ID : [CSCus65862](#)

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 AnyConnect Secure Mobility Client for Windowsの脆弱性により、認証されたローカルの攻撃者が、Microsoft Windowsオペレーティングシステムの SYSTEMアカウントと同等の権限で任意の実行可能ファイルをインストールして実行する可能性があります。

この脆弱性は、インストールされるファイルのパスとファイル名をコードでチェックできないことに起因します。攻撃者は、特別に変更されたINFファイルを作成することにより、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者は SYSTEMアカウントと同等の権限を使用して、基盤となるMicrosoft Windowsホストでコマンドを実行できる可能性があります。

シスコはこの脆弱性を確認し、ソフトウェアアップデートをリリースしました。

この脆弱性をエクスプロイトするには、攻撃者は認証を行い、ターゲットシステムへのローカルアクセスを持つ必要があります。これらの要件により、不正利用が成功する可能性が低下する可能性があります。

この脆弱性の影響を受けるのは、Microsoft Windowsオペレーティングシステムに該当するアプリケーションがインストールされている場合のみです。

シスコは、この脆弱性を報告していただいたGoogleセキュリティチームのKostya Kortchinsky氏に感謝いたします。

該当製品

シスコは登録ユーザ向けにBug ID [CSCus65862](#)をリリースしました。このBug IDには追加情報と、影響を受ける製品バージョンの最新リストが含まれています。

脆弱性のある製品

このアラートが最初に公開された時点では、Cisco AnyConnectセキュアモバイルクライアント3.1(60)には脆弱性が存在していました。Cisco AnyConnectセキュアモバイルクライアントの新しいリリースにも脆弱性が存在する可能性があります。

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

適切なアップデートを適用することを推奨します。

信頼できるユーザだけがローカルシステムにアクセスできるようにすることを推奨します。

管理者は、特権を持つユーザだけに管理システムまたは管理システムへのアクセスを許可することを推奨します。

影響を受けるシステムを監視することを推奨します。

修正済みソフトウェア

有効な契約を結んでいるシスコのお客様は、[Cisco](#)のSoftware Centerからアップデートを入手できます。契約を結んでいないシスコのお客様は、Cisco Technical Assistance Center(TAC)に1-800-553-2447または1-408-526-7209で連絡するか、tac@cisco.comで電子メールを介してアップグレードを入手できます。

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。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20150623-CVE-2015-4211>

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	初版リリース	適用外	Final	2015年6月 23日

利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザー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。