Cisco AnyConnect プロファイル エディタ XML 外部 エンティティ インジェクト脆弱性

Medium	**アドバイザリーID :** cisco-sa-20180117-acpe **初公開日 :** 2018-01-17 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 4.4 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvg19341	CVE-2018-0100

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 セキュア モビリティ クライアントのプロファイル エディタの脆弱性は非認証の、ローカル攻撃者が影響を受けたシステムの保存されている情報に読み書きアクセスがあることを可能にする可能性があります。

脆弱性は XML ファイルを解析するとき XML 外部 エンティティ（XXE）エントリの不適当な処理が原因です。 攻撃者は攻撃者がファイルを読み込み、書くことを可能にする可能性がある悪意のあるエントリが付いている巧妙に細工された XML ファイルのインジェクトによってこの脆弱性を不正利用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。
117-acpe

該当製品

脆弱性のある製品

この脆弱性は Cisco AnyConnect VPN Client ソフトウェアに影響を与えます。 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、この状況報告の上で 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やその公表を確認していません。

出典

Cisco はこの脆弱性を報告するために不眠症セキュリティのアラン Homewood に感謝することを望みます。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180117-acpe

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2018-January-17

利用規約

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。