Cisco Secure Access Control Server 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-20180307-acs **初公開日 :** 2018-03-07 16:00 **最終更新日 :** 2018-03-27 16:15 **バージョン 1.1 :** Final **CVSSスコア :** 5.3 **回避策 :** No workarounds available **Cisco バグ ID :** CSCve70595	CVE-2018-0207

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 Secure Access Control Server の Webベース ユーザインターフェイスの脆弱性はリモート攻撃者非認証が影響を受けたシステムのある特定の情報に *読み取り アクセス*を得るようにする可能性があります。

脆弱性は XML 外部 エンティティ (XXEs) の不適当な処理が原因 XML ファイルを解析するときです。 攻撃者は影響を受けたシステムの管理者の巧妙に細工された XML ファイルをインポートするように確信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。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180307-acs

該当製品

脆弱性のある製品

パブリケーションの時に、この脆弱性は 5.8 パッチ以前影響を受けた Cisco Secure Access Control Server 9.リリースします。 該当するソフトウェア リリースについての最新情報およびほとんどの詳細な情報に関しては、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

パブリケーションの時に、リリース 5.8 パッチ 9 はこの脆弱性のための修正が含まれていました。 修正済みソフトウェアリリースについての最新情報およびほとんどの詳細な情報に関しては、この状況報告の上で Cisco バグ ID を参照して下さい。

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

この脆弱性を発見して報告いただいた Positive Technologies 社のセキュリティ研究者、Mikhail Klyuchnikov 氏と Yury Aleynov 氏に謝意を表します。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180307-acs

改訂履歴

Version	Description	Section	Status	日付
1.1	この脆弱性を検出し、報告した信じられた研究者。	Source	Final	2018-March-27
1.0	初回公開リリース		Final	2018 年 3 月 7 日

利用規約

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。