Cisco Catalyst 4000 シリーズ スイッチ ダイナミック ACL バイパス の 脆弱性

Medium	**アドバイザリーID :** cisco-sa-20170906-cat **初公開日 :** 2017-09-06 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 4.7 **回避策 :** Yes **Cisco バグ ID :** CSCvc72751	CVE-2017-12213

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

動作する Cisco IOS XE ソフトウェアのダイナミック Access Control List （ ACL ） 機能の脆弱性は on Cisco 失敗します開いた Catalyst 4000 スイッチ非認証、隣接した攻撃者によりダイナミック ACL 割り当て失敗するためにおよびポートはことを可能にする可能性があります。 これは攻撃者が影響を受けたポートのデフォルトVLAN にトラフィックを通過させることを可能にする可能性があります。

脆弱性は 802.1X 認証が失敗した後スイッチポートに auth デフォルト *ACL* ダイナミック ACL の再割当の間に発生するかもしれない uncaught エラー状態が原因です。 この問題の正常なエクスプロイトは開いた物理的に隣接した攻撃者が 802.1X 認証をバイパスし、影響を受けたポートを失敗させますことを可能にする可能性がありま、影響を受けたスイッチポートのデフォルト VLAN にトラフィックを通過させることを攻撃者を許可します。

この脆弱性に対処する回避策があります。

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-20170906-cat

該当製品

修正済みソフトウェア

この脆弱性は on Cisco 動作する Cisco IOS XE ソフトウェアに Catalyst 4000 スイッチ影響を与えます。 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。

改訂履歴

Version	Description	Section	Status	日付
1.0	Initial public release.		Final	2017-September-06

利用規約