Cisco NX-OS システム ソフトウェア マネージメントインターフェイス サービス拒否の脆弱性

Medium	**アドバイザリーID :** cisco-sa-20180117-nxos **初公開日 :** 2018-01-17 16:00 **最終更新日 :** 2018-01-19 21:29 **バージョン 1.1 :** Final **CVSSスコア :** 5.3 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvf31132	CVE-2018-0090

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 NX-OS システム ソフトウェアのマネージメントインターフェイス Access Control List（ACL）設定の脆弱性はリモート攻撃者非認証がマネージメントインターフェイスの設定された ACL をバイパスするようにする可能性があります。 これはトラフィックが処理のための NX-OS CPU に転送されるようにする可能性がありま CPU使用率が高い状態およびサービス拒否（DoS）状態に導きます。

脆弱性はマネージメントインターフェイスにトラフィックが誤って分類されるようにし、適切な設定された ACL を一致する可能性がある 7.3.2 コード列の悪いコード修正が原因です。 攻撃者はマネージメントインターフェイスへ巧妙に細工されたトラフィックを送信 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。 エクスプロイトは攻撃者が設定されたマネージメントインターフェイス ACL をバイパスし、DoS 状態に終って目標とされたデバイスの CPU に、影響を与えることを可能に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-nxos

該当製品

脆弱性のある製品

この脆弱性は Cisco NX-OS システム ソフトウェアを実行する以下のシスコ製品に影響を及ぼします:

- マルチレイヤ ディレクタ スイッチ
- Nexus 2000 シリーズ スイッチ
- Nexus 3000 シリーズ スイッチ
- Nexus 5500 プラットフォーム スイッチ
- Nexus 5600 プラットフォーム スイッチ
- Nexus 6000 シリーズ スイッチ
- Nexus 7000 シリーズ スイッチ
- Nexus 7700 シリーズ スイッチ

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。

以下のシスコ製品はこの脆弱性から影響を受けません:

- Firepower 2100 シリーズ
- Firepower 4100 シリーズ次世代ファイアウォール
- Firepower 9300 セキュリティ アプライアンス
- Nexus 1000V シリーズ スイッチ
- Nexus 1100 シリーズ クラウド サービス プラットフォーム
- Nexus 3500 プラットフォーム スイッチ
- Nexus 3600 プラットフォーム スイッチ
- スタンドアロン NX-OS モードの Nexus 9000 シリーズ スイッチ
- シスコ アプリケーション セントリック インフラストラクチャ（ACI）モードの Nexus 9000 シリーズ ファブリックスイッチ
- Nexus 9500 R シリーズ ラインカードおよびファブリック モジュール
- ユニファイド コンピューティング システム（UCS）6100 シリーズ ファブリック インターコネクト
- UCS 6200 シリーズ ファブリック インターコネクト
- UCS 6300 シリーズ ファブリック インターコネクト

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

本脆弱性は、シスコ TAC のサポート案件の対応時に発見されました。

URL

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

改訂履歴

Version	Description	Section	Status	日付
1.1	脆弱からない脆弱なプロダクト リストに移られるスタンドアロン NX-OS モードの Nexus 9000 シリーズ スイッチ。	脆弱性が存在する製品、脆弱性が存在しない製品	Final	2018-January-19
1.0	初回公開リリース		Final	2018-January-17

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。