Cisco NX-OS ソフトウェアのロールベース アクセス コントロールにおける昇格権限の脆弱性

High

アドバイザリーID : cisco-sa-20180620-nxosrbac

初公開日 : 2018-06-20 16:00

最終更新日 : 2018-07-05 21:11

バージョン 1.1 : Final

CVSSスコア : 8.8

回避策 : No workarounds available

Cisco バグ ID : CSCvd77904

CVE-2018-0293

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 ソフトウェアのロールベース アクセス コントロール (RBAC) における脆弱性により、認証されたリモート攻撃者が、管理者以外のユーザに対しては制限しておく必要のある CLI コマンドを実行する可能性があります。 攻撃者は、デバイスの有効なユーザ クレデンシャルを保有する必要があります。

本脆弱性は、特定の CLI コマンドの RBAC 権限の割り当てが間違っていることに起因しています。 デバイスに対して管理者以外のユーザとして認証され、CLI から特定のコマンドが実行されると、本脆弱性がエクスプロイトされる危険性があります。 エクスプロイトが成功すると、管理ユーザに限定される必要があるコマンドが実行される可能性があります。 これらのコマンドは、デバイス上の設定やブート イメージを変更できます。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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-20180620-nxosrbac

このアドバイザリは、2018 年 6 月に公開された Cisco FXOS および NX-OS ソフトウェアのセキュリティ アドバイザリ コレクションの一部です。この中には、24 件の脆弱性に関する 24 件のシスコ セキュリティ アドバイザリが含まれています。 これらのアドバイザリとリンクの一覧については、以下を参照してください。Cisco Event Response: 2018 年 6 月 Cisco FXOS および NX-OS ソフトウェアのセキュリティ アドバイザリ コレクション

該当製品

脆弱性のある製品

本脆弱性は、Cisco NX-OS ソフトウェアの脆弱性のあるリリースを実行する次のシスコ製品に影響を与えます。

- MDS 9000 シリーズ マルチレイヤ 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 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
- 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
- スタンドアロン NX-OS モードの Nexus 9000 シリーズ 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

脆弱性が存在する Cisco NX-OS ソフトウェア リリースについては、このアドバイザリの「修正済みソフトウェア」の項を参照してください。

NX-OS デバイスの脆弱性の確認

特定の CLI コマンドについて設定されているユーザ ロールが *network-operator* の場合、攻撃者は、*network-admin* ロールのみに限定される必要のある CLI コマンドを実行する可能性があります。 管理者は、**show user-account** コマンドを使用して、各ユーザに関連付けられているロールを確認できます。

```
switch(config)# show user-account
user:admin
        this user account has no expiry date
        roles:network-admin
user:test
        this user account has no expiry date
        roles:network-operator
```

デバイスのロールとその適用の仕組みについては、NX-OS のマニュアルの「ユーザ ロールについて」を参照してください。

Cisco NX-OS ソフトウェア リリースの判別

管理者は、デバイスの CLI で **show version コマンド**を使用することによって、デバイスで実行されている Cisco NX-OS ソフトウェアのリリースをチェックできます。 デバイスが Cisco

NX-OS ソフトウェア リリース 7.3(2)D1(1) を実行している場合、コマンドの出力例は次のようになります。

```
nxos-switch# show version

Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Documents: http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html
Copyright (c) 2002-2017, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
Software
  BIOS:      version 2.12.0
  kickstart: version 7.3(2)D1(1)
  system:    version 7.3(2)D1(1)
.
.
.
```

脆弱性を含んでいないことが確認された製品

このアドバイザリの脆弱性のある製品セクションに記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- 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 9000 シリーズ ファブリック スイッチ (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)
- 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

Cisco では、本脆弱性が Cisco Nexus 4000 シリーズ スイッチ、Cisco Nexus 5010 スイッチ、Cisco Nexus 5020 スイッチに影響するかどうかを調査していません。これらの製品がサポート終了ステータスに達しているためです。 詳細については、「IBM BladeCenter 用の Cisco Nexus 4000 シリーズ スイッチ モジュールの販売終了およびサポート終了通知」および「Cisco Nexus 5010 および Nexus 5020 スイッチの販売終了およびサポート終了通知」を参照し

てください。

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

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。 お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。 そのようなソフトウェア アップグレードをインストール、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、お客様は以下のリンクに記載されたシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。 https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。 通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。 無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

この項の該当する表に示すように、適切なリリースにアップグレードすることをお勧めします。このアドバイザリはコレクションの一部です。これらも考慮した上、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。 コレクションに含まれるアドバイザリとリンクの一覧については、次を参照してください。シスコのイベント対応： 2018 年 6 月 Cisco FXOS および NX-OS ソフトウェアのセキュリティ アドバイザリ コレクション

次の表では、左の列に Cisco FXOS または NX-OS ソフトウェアのリリースを示しています。 中央の列は、リリースがこのアドバイザリに記載されている脆弱性に該当するかどうか、および、この脆弱性に対する修正を含む最初のリリースを示しています。 右の列は、リリースがこのアドバイザリ集に記載された何らかの脆弱性に該当するかどうか、および、それらすべての脆弱性に対する修正を含む最初のリリースを示しています。

MDS 9000 シリーズ マルチレイヤ スイッチ： CSCvd77904

Cisco NX-OS ソフトウェア リリース	この脆弱性に対する最初の修正リリース	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories
5.2	8.1(1)	8.1(1a) 8.2(1)
6.2	8.1(1)	8.1(1a) 8.2(1)
7.3	8.1(1)	8.1(1a) 8.2(1)
8.1	脆弱性なし	8.1(1a) 8.2(1)
8.2	脆弱性なし	脆弱性なし

Nexus 3000 シリーズ スイッチ： CSCvd77904

Cisco NX-OS ソフトウェア リリース	この脆弱性に対する最初の修正リリース	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories
7.0(3)I4 よりも前	7.0(3)I4(7)	7.0(3)I7(4)
7.0(3)I4	7.0(3)I4(7)	7.0(3)I7(4)
7.0(3)I5	7.0(3)I7(1)	7.0(3)I7(4)
7.0(3)I6	7.0(3)I7(1)	7.0(3)I7(4)
7.0(3)I7	7.0(3)I7(1)	7.0(3)I7(4)

Nexus 3500 プラットフォーム スイッチ： CSCvd77904

Cisco NX-OS ソフトウェア リリース	この脆弱性に対する最初の修正リリース	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories
6.0	脆弱性なし	7.0(3)I7(4)
7.0	7.0(3)I7(2)	7.0(3)I7(4)

Nexus 2000、5500、5600、6000 シリーズ スイッチ： CSCvd77904

Cisco NX-OS ソフトウェア リリース	この脆弱性に対する最初の修正リリース	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories
6.0	7.3(3)N1(1)	7.3(3)N1(1)

7.0	7.3(3)N1(1)	7.3(3)N1(1)
7.1	7.3(3)N1(1)	7.3(3)N1(1)
7.2	7.3(3)N1(1)	7.3(3)N1(1)
7.3	7.3(3)N1(1)	7.3(3)N1(1)

Nexus 7000 および 7700 シリーズ スイッチ CSCvd77904

Cisco NX-OS ソフトウェア リリース	この脆弱性に対する最初の修正リリース	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories
6.2	7.3(2)D1(1)	8.1(2) または 8.2(1)
7.2	7.3(2)D1(1)	8.1(2) または 8.2(1)
7.3	7.3(2)D1(1)	8.1(2) または 8.2(1)
8.0	8.1(1)	8.1(2) または 8.2(1)
8.1	脆弱性なし	8.1(2) または 8.2(1)
8.2	脆弱性なし	8.1(2) または 8.2(1)

スタンドアロン NX-OS モードの Nexus 9000 シリーズ スイッチ： CSCvd77904

Cisco NX-OS ソフトウェア リリース	この脆弱性に対する最初の修正リリース	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories
7.0(3)I4 よりも前	7.0(3)I4(7)	7.0(3)I7(4)
7.0(3)I4	7.0(3)I4(7)	7.0(3)I7(4)
7.0(3)I5	7.0(3)I7(1)	7.0(3)I7(4)
7.0(3)I6	7.0(3)I7(1)	7.0(3)I7(4)
7.0(3)I7	7.0(3)I7(1)	7.0(3)I7(4)

Nexus 9500 R シリーズ向けライン カードおよびファブリック モジュール、Nexus 3600 プラットフォーム スイッチ: CSCvd77904

Cisco NX-OS ソフトウェア リリース	この脆弱性に対する最初の修正リリース	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories
7.0	7.0(3)F1(1)	7.0(3)F3(3a)

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、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180620-nxosrbac

改訂履歴

Version	Description	Section	Status	日付
1.1	MDS	修正済みソフトウェア	Final	2018 年 7 月 5 日
1.0	初回公開リリース		Final	2018 年 6 月 20 日

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。