Cisco NX-OS ソフトウェアにおける特権昇格の脆弱性

アドバイザリーID : cisco-sa-20190306-nxos-escalation
初公開日 : 2019-03-06 16:00
バージョン 1.0 : Final
CVSSスコア : 7.8
回避策 : No workarounds available
Cisco バグ ID : CSCvj59009 CSCvk70659

CVE-2019-1602

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 ソフトウェアのファイルシステム権限の脆弱性により、認証されたローカル攻撃者が管理者への特権の昇格に使用することが可能な機密データにアクセスできるようになります。

この脆弱性は、ファイルシステム権限が適切に実装されていないことに起因しています。攻撃者は、該当デバイスの CLI にログインして特定のファイルにアクセスし、その情報を活用して NX-API サーバの認証を行うことにより、この脆弱性をエクスプロイトする可能性があります。エクスプロイトが成功すると、攻撃者は管理者として設定を変更できるようになります。

注:NX-APIはデフォルトで無効になっています。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-escalation

このアドバイザリは、2019 年 3 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 バンドルの一部です。このバンドルの中には、26 件の脆弱性に関する 25 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。アドバイザリの完全なリストとそのリンクについては、『Cisco Event Response: March 2019 Cisco FXOS and NX-OS Software Security Advisory Bundled Publication』を参照してください。

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。

- 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
- 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。

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 7.0(3)I5(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
Copyright (C) 2002-2016, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source.  This software is provided "as is," and
unless otherwise stated, there is no warranty, express or implied,
including but not limited to warranties of merchantability and fitness
for a particular purpose. Certain components of this software are
licensed under the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
Software
  BIOS: version 07.57
  NXOS: version 7.0(3)I5(1) [build 7.0(3)I5(0.9)]
  BIOS compile time:  06/29/2016
  NXOS image file is: bootflash:///nxos.7.0.3.I5.0.9.bin
  NXOS compile time:  8/1/2016 23:00:00 [08/02/2016 00:30:32]
  .
  .
  .
```

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製品
- Firepower 9300 セキュリティ アプライアンス
- MDS 9000 シリーズ マルチレイヤ スイッチ
- Nexus 1000V Switch for Microsoft Hyper-V
- Nexus 1000V Switch for VMware vSphere
- Nexus 2000 シリーズ ファブリック エクステンダ
- 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
- 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 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
- UCS 6400 シリーズ ファブリック インターコネクト

詳細

この脆弱性は、NX-API 機能が有効に設定されている Cisco NX-OS ソフトウェアを実行中のデバイスにのみ影響を与えます。

Cisco NX-OS ソフトウェアを実行するデバイスで NX-API が有効に設定されているかどうかを判断するにあたっては、管理者が Cisco NX-OS の CLI から show feature | include nxapi コマンドを NX-OS の CLI から使用して、有効になっていることを確認します。次の例は、Cisco NX-OS ソフトウェアを実行するデバイスで NX-API 機能が有効になっていることを示しています。

```
nxos-switch# show feature | include nxapi
             nxapi                 1        enabled
```

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リリースしています。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、アクセスまたはその他の方法で使用した場合、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、[シスコのセキュリティアドバイザリおよびアラート（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 Cisco Service Contract 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 POS 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。完全なアップグレード ソリューションを確認するにあたっては、このアドバイザリが公開されたバンドルの一部であることを考慮する必要があります。次のページに、バンドルアドバイザリの完全なリストがあります。Cisco Event Response: March 2019 Cisco FXOS and NX-OS Software Security Advisory Bundled Publication。

次の表では、左の列に Cisco FXOS ソフトウェアまたは Cisco 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、リリースがこのバンドルに記載されたすべての脆弱性の影響を受けるかどうか、およびどのリリースにそれらの脆弱性に対する修正が含まれているのかを示しています。

各表の右の列に記載されているリリースには、脆弱性に対する修正が含まれていますが、Cisco NX-OS ソフトウェアのイメージ署名検証の脆弱性に関連する修正については、ソフトウェア アップグレードの一部として BIOS をアップグレードする必要があります。以下に示すいずれかの製品のソフトウェアをアップグレードする場合は、このアドバイザリに記載されている BIOS アップグレードと、該当製品の ID および BIOS バージョンの詳細を参照することをお勧めします。

- Nexus 3000 シリーズ スイッチ
- ACI モードの Nexus 9000 シリーズ ファブリック 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

Nexus 3000シリーズスイッチ：CSCvj59009

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	アドバイザリのバンドルに記載されているすべての脆弱性に対する最初の修正済みリリース
7.0(3)I4 よりも前	脆弱性なし	7.0(3)I7(6)
7.0(3)I4	脆弱性なし	7.0(3)I7(6)
7.0(3)I5	7.0(3)I7(4)	7.0(3)I7(6)
7.0(3)I6	7.0(3)I7(4)	7.0(3)I7(6)
7.0(3)I7	7.0(3)I7(4)	7.0(3)I7(6)
9.2	脆弱性なし	9.2(2)

Nexus 3500プラットフォームスイッチ：CSCvj59009

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	アドバイザリのバンドルに記載されているすべての脆弱性に対する最初の修正済みリリース
6.0	脆弱性なし	6.0(2)A8(11)
7.0(3)	7.0(3)I7(4)	6.0(2)A8(11)
9.2(1)	脆弱性なし	9.2(2)

Nexus 3600プラットフォームスイッチ：CSCvk70659

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	アドバイザリのバンドルに記載されているすべての脆弱性に対する最初の修正済みリリース
7.0(3)F3	7.0(3)F3(3c)[1]	7.0(3)F3(5)
9.2(1)	脆弱性なし	9.2(2)

1この脆弱性は、7.0(3)F3(4) では修正されていませんが、7.0(3)F3(5) で修正されています。

スタンドアロンNX-OSモードのNexus 9000シリーズスイッチ：CSCvj59009

Cisco NX-OS ソフトウェア	この脆弱性に対する最初の修正リリース	アドバイザリのバンドルに記載されているすべての脆弱性に対する最初の修正済みリリース
7.0(3)I4 よりも前	脆弱性なし	7.0(3)I7(6)
7.0(3)I4	脆弱性なし	7.0(3)I7(6)
7.0(3)I5	7.0(3)I7(4)	7.0(3)I7(6)
7.0(3)I6	7.0(3)I7(4)	7.0(3)I7(6)
7.0(3)I7	7.0(3)I7(4)	7.0(3)I7(6)
9.2	脆弱性なし	9.2(2)

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：CSCvk70659

Cisco NX-OS ソフトウェア	この脆弱性に対する最初の修正リリース	アドバイザリのバンドルに記載されているすべての脆弱性に対する最初の修正済みリリース
7.0(3)F1	7.0(3)F3(3c)[1]	7.0(3)F3(5)
7.0(3)F2	7.0(3)F3(3c)[1]	7.0(3)F3(5)
7.0(3)F3	7.0(3)F3(3c)[1]	7.0(3)F3(5)
9.2(1)	脆弱性なし	9.2(2)

1この脆弱性は、7.0(3)F3(4) では修正されていませんが、7.0(3)F3(5) で修正されています。

関連情報

Cisco Nexus スイッチに最適な Cisco NX-OS ソフトウェア リリースの決定に関してサポートが必要な場合は、以下の推奨リリースに関するドキュメントを参照してください。 セキュリティ アドバイザリでより新しいリリースが推奨されている場合は、そのアドバイザリのガイダンスに従うことをお勧めします。

Cisco MDS シリーズ スイッチ
VMware 向け Cisco Nexus 1000V スイッチ
Cisco Nexus 3000 シリーズおよび 3500 シリーズ スイッチ

Cisco Nexus 5000 Series Switches
Cisco Nexus 5500 プラットフォーム スイッチ
Cisco Nexus 6000 Series Switches
Cisco Nexus 7000 Series Switches
Cisco Nexus 9000 Series Switches
ACI モードの Cisco Nexus 9000 シリーズ スイッチ

Cisco UCS に最適な Cisco NX-OS ソフトウェア リリースの確認に関してサポートが必要な場合は、デバイスのリリース ノートに記載されている推奨リリースに関するドキュメントを参照してください。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、本アドバイザリに記載されている脆弱性の不正利用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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190306-nxos-escalation

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2019 年 3 月 6 日

利用規約

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。