Cisco NX-OS ソフトウェアの CLI におけるコマンド インジェクションに関する脆弱性 (CVE-2019-1612)

High

アドバイザリーID : cisco-sa-20190306-nxos-cmdinj-1612

初公開日 : 2019-03-06 16:00

バージョン 1.0 : Final

CVSSスコア : 4.2

回避策 : No workarounds available

Cisco バグ ID : CSCvj12009 CSCvi42373

CVE-2019-1612

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 CLI における脆弱性により、認証されたローカル攻撃者が、該当デバイスの OS 上で任意のコマンドを実行できるようになります。

この脆弱性は、特定の CLI コマンドに渡される引数が十分に検証されないことに起因しています。 攻撃者が、該当コマンドの引数として悪意のある入力を含めることにより、この脆弱性をエクスプロイトする可能性があります。 エクスプロイトに成功すると、攻撃者は、昇格された特権を使用して OS 上で任意のコマンドを実行可能になります。 攻撃者がこの脆弱性をエクスプロイトするには、有効な管理者クレデンシャルが必要です。

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ました。 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-20190306-nxos-cmdinj-1612

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。 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。 シスコのイベント対応： 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。

このバンドルには、CLI のコマンド インジェクションに関する類似した脆弱性がいくつか記載されています。 それらの主な相違点は、影響を受ける製品やソフトウェア バージョンにあります。 詳細については、「詳細」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が存在する製品のセクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

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 ファイアウォール
- 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

このバンドルには、CLI のコマンド インジェクションに関する類似した脆弱性がいくつか記載されています。 それらの主な相違点は、影響を受ける製品やソフトウェア バージョンにあります。次の表では、セキュリティ アドバイザリ タイトルで使用されている不具合 ID と CVE ID が割り振られた各脆弱性と、それらの影響を受ける製品を示します。

セキュリティ アドバイザリ	FP 4100/9300	N3K/N9K	N3500	N2K/N5K/N6K	MDS/N7K	N3600/N9500R
Cisco NX-OS ソフトウェアの CLI におけるコマンド インジェクションに関する脆弱性（CVE-2019-1606）	N/A	CSCvh85760	CSCvh85760	N/A	N/A	N/A
Cisco NX-OS ソフトウェアの CLI	N/A	N/A	N/A	N/A	CSCvi0	N/A

におけるコマンド インジェクションに関する脆弱性（CVE-2019-1607）					1416[1]	
Cisco NX-OS ソフトウェアの CLI におけるコマンド インジェクションに関する脆弱性（CVE-2019-1608）	N/A	N/A	N/A	N/A	CSCvi01422	N/A
Cisco NX-OS ソフトウェアの CLI におけるコマンド インジェクションの脆弱性（CVE-2019-1609）	N/A	CSCvj63253	CSCvj63253	N/A	CSCvk51388	CSCvk51387
Cisco NX-OS ソフトウェアの CLI におけるコマンド インジェクションに関する脆弱性（CVE-2019-1610）	N/A	CSCvj61991[2]	CSCvj61991	N/A	N/A	N/A
Cisco NX-OS および FXOS ソフトウェアの CLI におけるコマンド インジェクションに関する脆弱性（CVE-2019-1611）	CSCvk65447	CSCvj65666	CSCvj65666	CSCvk65444	CSCvj63798	CSCvk65482
Cisco NX-OS ソフトウェアの CLI におけるコマンド インジェクションに関する脆弱性（CVE-2019-1612）	N/A	CSCvi42373	CSCvi42373	N/A	N/A	CSCvj12009
Cisco NX-OS ソフトウェアの CLI におけるコマンド インジェクションに関する脆弱性（CVE-2019-1613）	N/A	CSCvj65654	CSCvk50906	N/A	CSCvj63807	CSCvk50903

[1]CSCvi01416 は、Nexus 7000 シリーズ スイッチにのみ適用されます。 MDS 9000 シリーズ マルチレイヤ スイッチは、この脆弱性の影響を受けません。
[2]CSCvj61991 は、Nexus 3000 シリーズ スイッチにのみ適用されます。 スタンドアロン NX-OS モードの Nexus 9000 シリーズ スイッチは、この脆弱性の影響を受けません。

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

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は新規リリースでも継続して適切なサポートが受けられることを確認してください。 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。 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。 バンドル アドバイザリの完全なリストは、次のページにあります。 シスコのイベント レスポンス： 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。

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。 右の列では、今回のアドバイザリ バンドルに記載された脆弱性全体に対する最初の修正リリースを、影響を受けるソフトウェア リリースごとに記載しています。

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 イメージの署名検証に関する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： CSCvi42373

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 バンドルに記載されている脆弱性全体に対する最初の修正リリース
7.0(3)I4 よりも前	7.0(3)I4(9)	7.0(3)I7(6)
7.0(3)I4	7.0(3)I4(9)	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： CSCvi42373

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 バンドルに記載されている脆弱性全体に対する最初の修正リリース
6.0(2)A8 より前	脆弱性なし	6.0(2)A8(11)
6.0(2)A8	脆弱性なし	6.0(2)A8(11)
7.0(3)	7.0(3)I7(4)	7.0(3)I7(6)
9.2	脆弱性なし	9.2(2)

Nexus 3600 プラットフォーム スイッチ： CSCvj12009

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 バンドルに記載されている脆弱性全体に対する最初の修正リリース
7.0(3)F3	7.0(3)F3(3c)[1]	7.0(3)F3(5)
9.2	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： CSCvi42373

Cisco NX-	この脆弱性に対する最初の修正	アドバイザリ バンドルに記載されている脆弱性全体

OS ソフトウェア リリース	リリース	に対する最初の修正リリース
7.0(3)I4 よりも前	7.0(3)I4(9)	7.0(3)I4(9)
7.0(3)I4	7.0(3)I4(9)	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： CSCvj12009

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 バンドルに記載されている脆弱性全体に対する最初の修正リリース
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	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 リリースの確認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 シリーズ スイッチ
Cisco Nexus 5500 プラットフォーム スイッチ
Cisco Nexus 6000 Series Switches
Cisco Nexus 7000 シリーズ スイッチ
Cisco Nexus 9000 シリーズ スイッチ
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）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-20190306-nxos-cmdinj-1612

改訂履歴

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

利用規約