Cisco FXOS および NX-OS ソフトウェア コマンド インジェクト脆弱性（CVE-2019-1780）

Medium	**アドバイザリーID：** cisco-sa-20190515-nxos-fxos-cmdinj-1780 **初公開日：** 2019-05-15 16:00 **最終更新日：** 2019-05-21 13:55 **バージョン 1.1：** Final **CVSSスコア：** 4.2 **回避策：** No workarounds available **Cisco バグ ID：** CSCvi92328 CSCvi01431 CSCvi92329 CSCvi92326 CSCvi01440 CSCvi92332	CVE-2019-1780

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 FXOS ソフトウェアおよび Cisco NX-OS ソフトウェアの CLI の脆弱性は管理者の資格情報が付いている高度な特権の影響を受けたデバイスの基礎オペレーティング システムの任意のコマンドを実行する認証された、ローカル攻撃者を可能にする可能性があります。

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。 エクスプロイトが成功すると、攻撃者は昇格された特権を使用して基盤となるオペレーティング システムで任意のコマンドを実行できるようになります。 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-20190515-nxos-fxos-cmdinj-1780

該当製品

脆弱性のある製品

この脆弱性は Cisco FXOS ソフトウェアまたは NX-OS ソフトウェアの脆弱なリリースを実行する場合以下のシスコ製品に影響を及ぼします:

- Firepower 4100 シリーズ
- 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 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 スイッチング プラットフォーム

脆弱性が存在する Cisco FXOS ソフトウェアおよび 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。

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
- Nexus 1000V Switch for Microsoft Hyper-V
- Nexus 1000V Switch for VMware vSphere
- 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

Cisco は複数の同じような CLI コマンド インジェクト脆弱性を表わしました。 それらは該当製品およびソフトウェア バージョンで主に異なります。 この表は Cisco バグ ID および CVE ID によって各脆弱性のための該当製品を示したものです。

セキュリティ アドバイザリ	FP 4100/ 9300	MDS 9K/ N7K/ N7700[1]	N1000V MS/VM	N3K/N3500/ N9K-NXOS	N3600/ N9500R	N5500K/ N5600/ N6K	UCS 6200/ UCS 6300 UCS 6400[2]
Cisco NX-OS ソフトウェア コマンド インジェクト脆弱性（CVE-2019-1735）	N/A	CSCvj63728	CSCvk52969 CSCvk52985	CSCvj63877 CSCvk52971	CSCvk52988	CSCvk52972	CSCvk52975
Cisco NX-OS ソフトウェア ラインカード コマンド インジェクト脆弱性（CVE-2019-1769）	N/A	N/A	N/A	CSCvh20032	CSCvj00299	N/A	N/A
Cisco NX-OS ソフトウェア コマンド インジェクト脆弱性（CVE-2019-1770）	N/A	CSCvh75867[1]	CSCvi92240 CSCvk36294	CSCvh75958 CSCvi92242	CSCvi92239	CSCvi92243	N/A
Cisco NX-OS ソフトウェア コマンド インジェクト脆弱性（CVE-2019-1774、CVE-2019-1775）	N/A	CSCvh75895 CSCvh75909	N/A	CSCvh75968 CSCvh75976 CSCvi99197 CSCvi92258	CSCvi99195 CSCvi92256	CSCvi99198 CSCvi92260	N/A
Cisco NX-OS ソフトウェア コマンド インジェクト脆弱性（CVE-2019-1776）	N/A	CSCvh20081	N/A	CSCvh20076 CSCvi96431	CSCvi96429	CSCvi96432	CSCvi96433[2]
Cisco NX-OS ソフトウェア コマンド インジェクト脆弱性（CVE-2019-1778）	N/A	N/A	N/A	CSCvh75996	CSCvj03877	N/A	N/A
Cisco FXOS および NX-OS ソフトウェア コマンド インジェクト脆弱性（CVE-2019-1779）	CSCvj00418	CSCve51688	N/A	CSCvh76126	CSCvj00412	CSCvj00416	N/A
Cisco FXOS および NX-OS ソフトウェア コマンド インジェクト脆弱性（CVE-2019-1780）	CSCvi92332	CSCvi01440	N/A	CSCvi01431 CSCvi92328	CSCvi92326	CSCvi92329	N/A
Cisco FXOS および NX-OS ソフトウェア コマンド インジェクト脆弱性（CVE-2019-1781、CVE-2019-1782）	CSCvi96527 CSCvi92130	CSCvi01448 CSCvh20389	N/A	CSCvi01445 CSCvh20027 CSCvi96524 CSCvi92126	CSCvi96522 CSCvi91985	CSCvi96525 CSCvi92128	CSCvi96526[2] CSCvi92129[2]
Cisco NX-OS ソフトウェア コマンド インジェクト脆弱性（CVE-2019-1783）	N/A	CSCvi42281[1]	N/A	N/A	N/A	CSCvj03966	N/A
Cisco NX-OS ソフトウェア コマンド インジェクト脆弱性（CVE-2019-1784）	N/A	CSCvi42292[1]	N/A	N/A	N/A	CSCvj12273	CSCvj12274[2]
Cisco NX-OS ソフトウェア コマンド インジェクト脆弱性（CVE-2019-1790）	N/A	CSCvh20112	N/A	CSCvh20096	CSCvi96504	CSCvi96509	CSCvi96510[2]
Cisco NX-OS ソフトウェア コマンド インジェクト脆弱性（CVE-2019-1791）	N/A	CSCvj63667	N/A	CSCvj63270	CSCvk50889	CSCvk50876	N/A

				CSCvk50873			
Cisco FXOS および NX-OS ソフトウェア コマンド インジェクト脆弱性（CVE-2019-1795）	CSCvh66259	CSCvh20359	CSCvh66257 CSCvk30761	CSCvh20029 CSCvh66219	CSCvh66202	CSCvh66214	CSCvh66243[2]

1. CSCvh75867、CSCvi42281 および CSCvi42292 は Nexus 7000 シリーズおよび Nexus 7700 シリーズだけスイッチに適用します。 MDS 9000 シリーズ マルチレイヤ スイッチはこれらの脆弱性から影響を受けません。
2. CSCvk52975 は UCS 6200、6300、および 6400 に適用します。 他のすべての UCS 問題に関しては、UCS だけ 6200 および 6300 影響を受けているです（および UCS 6400 は影響を受けていません）。

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

アップグレード アクションは行進 2019 Cisco FXOS をおよび NX-OS ソフトウェア 当たるために顧客が既に推奨される Cisco NX-OS ソフトウェア リリースをバンドル加えてしまったケースのための Cisco NX-OS ソフトウェアを実行している製品に必要ではないです。 Cisco イベント応答が表示されて下さい: 行進 2019 Cisco FXOS および NX-OS ソフトウェア Security Advisory はバンドルのアドバイザリのリストのためのパブリケーションを組み込みました。

行進に 2019 のバンドルを当たるために推奨されるリリースを加えないか、または Cisco FXOS ソフトウェアを実行しているデバイスがある顧客はこのセクションの適当な表に示すように適切なリリースにアップグレードするように勧告されます。 次の表では、左の列は Cisco FXOS および NX-OS ソフトウェア リリースをリストします。 右の列はこの脆弱性のための修正を含む最初のリリースを示します。

Firepower 4100 シリーズおよび Firepower 9300 セキュリティ アプライアンス: CSCvi92332

Cisco FXOS 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
2.3 より前	2.3.1.130
2.3	2.3.1.130
2.4	2.4.1.122

MDS 9000 シリーズ マルチレイヤ スイッチ： CSCvi01440

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
5.2	6.2(25)
6.2	6.2(25)
7.3	8.1(1b)
8.1	8.1(1b)
8.2	8.2(3)
8.3	8.3(1)

スタンドアロン NX-OS モードの Nexus 3000 シリーズ スイッチおよび Nexus 9000 シリーズ スイッチ： CSCvi01431

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

7.0(3)I4 よりも前	7.0(3)I4(9)
7.0(3)I4	7.0(3)I4(9)
7.0(3)I7	7.0(3)I7(4)
9.2(1)	脆弱性なし

Nexus 3500 プラットフォーム スイッチ： CSCvi92328

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
6.0(2)A8 より前	6.0(2)A8(11)
6.0(2)A8	6.0(2)A8(11)
7.0(3)I4	7.0(3)I4(9)
7.0(3)I7	7.0(3)I7(4)
9.2	脆弱性なし

Nexus 3600 プラットフォーム スイッチおよび Nexus 9500 R シリーズ スイッチング プラットフォーム: CSCvi92326

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
7.0(3)	7.0(3)F3(5)
9.2	脆弱性なし

Nexus 5500 および 5600 プラットフォーム スイッチおよび 6000 シリーズ スイッチ: CSCvi92329

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
7.3 前	7.3(3)N1(1)
7.3	7.3(3)N1(1)

Nexus 7000 および 7700 シリーズ スイッチ CSCvi01440

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
6.2 より前	6.2(22)
6.2	6.2(22)
7.2	7.3(3)D1(1)
7.3	7.3(3)D1(1)
8.0	8.2(3)
8.1	8.2(3)
8.2	8.2(3)
8.3	8.3(1)

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 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-20190515-nxos-fxos-cmdinj-1780

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.1	Nexus 3000 シリーズ スイッチおよび Nexus 9000 シリーズ スイッチによって修復されたリリース表を更新しました。	修正済みソフトウェア	最終版	2019-May-21
1.0	初回公開リリース		最終版	2019-May-15

利用規約

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。