

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)

Medium	アドバイザーID : cisco-sa-20190515-nxos-fxos-cmdinj-1779	CVE-2019-1779
	初公開日 : 2019-05-15 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 : CSCvj00416	
	CSCvj00418 CSCve51688	
	CSCvj00412 CSCvh76126	

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。攻撃者は有効なデバイス 資格情報がこの脆弱性を不正利用することを必要とします。

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。

このアドバイザーは、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-1779>

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/N35 00/ 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	CSCvj63 728	CSCvk52 969 CSCvk52 985	CSCvj63 877 CSCvk52 971	CSCvk52 988	CSCvk52 972	CSCvk52 975
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	CSCvh20 032	CSCvj00 299	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	CSCvh75 867 ¹	CSCvi92 240 CSCvk36 294	CSCvh75 958 CSCvi92 242	CSCvi92 239	CSCvi92 243	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	CSCvh75 895 CSCvh75 909	N/A	CSCvh75 968 CSCvh75 976 CSCvi99 197 CSCvi92 258	CSCvi99 195 CSCvi92 256	CSCvi99 198 CSCvi92 260	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	CSCvh20 081	N/A	CSCvh20 076 CSCvi96 431	CSCvi96 429	CSCvi96 432	CSCvi96 433 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	CSCvh75 996	CSCvj03 877	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)	CSCvj00 418	CSCve51 688	N/A	CSCvh76 126	CSCvj00 412	CSCvj00 416	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)	CSCvi92 332	CSCvi01 440	N/A	CSCvi01 431 CSCvi92 328	CSCvi92 326	CSCvi92 329	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)	CSCvi96 527 CSCvi92 130	CSCvi01 448 CSCvh20 389	N/A	CSCvi01 445 CSCvh20 027 CSCvi96 524 CSCvi92 126	CSCvi96 522 CSCvi91 985	CSCvi96 525 CSCvi92 128	CSCvi96 526 ² CSCvi92 129 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	CSCvi42 281 ¹	N/A	N/A	N/A	CSCvj03 966	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	CSCvi42 292 ¹	N/A	N/A	N/A	CSCvj12 273	CSCvj12 274 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	CSCvh20 112	N/A	CSCvh20 096	CSCvi96 504	CSCvi96 509	CSCvi96 510 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	CSCvj63 667	N/A	CSCvj63 270 CSCvk50 873	CSCvk50 889	CSCvk50 876	N/A
Cisco FXOS および NX-OS ソフトウェア コ	CSCvh66	CSCvh20	CSCvh66	CSCvh20	CSCvh66	CSCvh66	CSCvh66

マンド インジェクト脆弱性 (CVE-2019-1795)	259	359	257 CSCvk30 761	029 CSCvh66 219	202	214	243 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 影響を受けています (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です。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 当てるために既に推奨されるリリースをバンドル加えてしまった顧客向けに必要なではありません。 [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 のバンドルを当てるために推奨されるリリースを加えなかった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: [CSCvj00418](#)

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
2.4 前	2.4.1.101
2.4	2.4.1.101

MDS 9000 シリーズ マルチレイヤ スイッチ : [CSCve51688](#)

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	8.3(1)
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、Nexus 3500 プラットフォーム スイッチおよび Nexus 9000 シリーズ スイッチ: [CSCvh76126](#)

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 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: [CSCvj00412](#)

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:

[CSCvj00416](#)

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(4)N1(1)
7.3	7.3(4)N1(1)

Nexus 7000 および 7700 シリーズ スイッチ [CSCve51688](#)

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	8.3(1)
8.1	8.3(1)
8.2	8.3(1)
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ーにより新しいリリースが推奨されている場合は、そのアドバイザー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-1779>

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-May-15

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、単独の転載や意識を施した場合、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。