Cisco FXOS、IOS XR、および NX-OS ソフトウェアの Cisco Discovery Protocol におけるサービス妨害の脆弱性

High

アドバイザリーID : cisco-sa-20200205-fxnxos-iosxr-cdp-dos

CVE-2020-3120

初公開日 : 2020-02-05 16:00

最終更新日 : 2020-02-21 20:46

バージョン 1.3 : Interim

CVSSスコア : 7.4

回避策 : No workarounds available

Cisco バグ ID : CSCvr15072 CSCvr15083 CSCvr15073 CSCvr15078 CSCvr15111 CSCvr15024 CSCvr15079 CSCvr14976 CSCvr15082

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、Cisco IOS XR ソフトウェア、および Cisco NX-OS ソフトウェアに実装された Cisco Discovery Protocol に存在する脆弱性により、近接する未認証の攻撃者が該当デバイスのリロードを引き起こし、その結果サービス妨害（DoS）状態が発生する可能性があります。

この脆弱性は、影響を受けるソフトウェアが Cisco Discovery Protocol のメッセージを処理するときにチェックが行われないことに起因します。この脆弱性は、該当デバイスに悪意のある Cisco Discovery Protocol パケットを送信することでエクスプロイトされる可能性があります。エクスプロイトに成功すると、攻撃者はシステムメモリを使い果たしてデバイスのリロードを引き起こせるようになります。

注：Cisco Discovery Protocol はレイヤ 2 プロトコルです。この脆弱性をエクスプロイトするには、攻撃者は該当デバイスと同じブロードキャストドメイン内に存在する（レイヤ 2 と隣接関係にある）必要があります。

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-20200205-fxnxos-iosxr-cdp-dos

該当製品

脆弱性のある製品

Cisco Discovery Protocol が 1 つ以上のインターフェイスでグローバルに有効になっており、Cisco FXOS、IOS XR（32 ビットまたは 64 ビット）、または NX-OS ソフトウェアの脆弱性のあるリリースを実行している場合、次のシスコ製品がこの脆弱性の影響を受けます。

- ASR 9000 シリーズ アグリゲーション サービス ルータ
- Carrier Routing System（CRS）
- Firepower 4100 シリーズ
- Firepower 9300 セキュリティ アプライアンス
- IOS XRv 9000 ルータ
- MDS 9000 シリーズ マルチレイヤ スイッチ
- Network Convergence System（NCS）540 シリーズ ルータ
- Network Convergence System（NCS）560 シリーズ ルータ
- Network Convergence System（NCS）1000 シリーズ
- Network Convergence System（NCS）5000 シリーズ
- Network Convergence System（NCS）5500 シリーズ
- Network Convergence System（NCS）6000 シリーズ
- VMware vSphere 向け Nexus 1000 Virtual Edge
- Nexus 1000V Switch for Microsoft Hyper-V
- Nexus 1000V Switch for VMware vSphere
- Nexus 3000 シリーズ 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 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）
- スタンドアロン NX-OS モードの Nexus 9000 シリーズ スイッチ
- 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

Cisco Discovery Protocol が 1 つ以上のインターフェイスでグローバルに有効になっており、Cisco IOS XR ソフトウェアの脆弱性のあるリリースを実行している場合、サードパーティの

ホワイトボックスルータもこの脆弱性の影響を受けます。

注：Cisco Discovery Protocol は、Cisco IOS XR ソフトウェアでデフォルトで無効になっています。Cisco Discovery Protocol はグローバルに、かつ Cisco FXOS および NX-OS ソフトウェアのすべてのインターフェイスでデフォルトで有効になっています。

脆弱性が存在する Cisco FXOS、IOS XR、および NX-OS ソフトウェアの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 FXOS ソフトウェアの Cisco Discovery Protocol の状態を確認する

Cisco Discovery Protocol は、管理（mgmt0）ポートで常に有効になっています。2.1 より前の Cisco FXOS ソフトウェアリリースでは、Cisco Discovery Protocol はすべての前面ポートでも常に有効化されています。

Cisco IOS XR ソフトウェアの Cisco Discovery Protocol のステータスを確認する

管理者は、デバイスの CLI で **show running-config | include cdp**コマンドを使用します。コマンドが少なくとも次の行を返す場合、Cisco Discovery Protocol はグローバルに、かつ 1 つ以上のインターフェイスで有効になっています。

```
RP/0/RP0/CPU0:ios#show running-config | include cdp
Mon Dec  2 17:00:27.921 UTC
Building configuration...
cdp
 cdp
.
.
.
```

Cisco NX-OS ソフトウェアを実行している Cisco Nexus スイッチ上の Cisco Discovery Protocol のステータスを確認する

管理者は、デバイスの CLI で **show running-config cdp all | include "cdp enable"**コマンドを使用します。コマンドが少なくとも次の行を返す場合、Cisco Discovery Protocol はグローバルに、かつ 1 つ以上のインターフェイスで有効になっています。

```
nxos#  show running-config cdp all | include "cdp enable"
cdp enable
  cdp enable
```

Cisco UCS ファブリック インターコネクト上の Cisco Discovery Protocol のステータスを確認する

Cisco Discovery Protocol は、イーサネット アップリンク ポート（ネットワーク接続用のアップストリームスイッチに接続するネットワーク インターフェイス）、イーサネット ポート チ

ャネル メンバー、FCoE アップリンクポート、および管理ポートで常に有効になっています。

管理者は、デバイスの CLI で **show configuration | egrep "^ scope|enable cdp"コマンドを**使用します。次の例に示すように、コマンドが **org 範囲で enable cdp コマンドを返す場合、 Cisco Discovery Protocol はサーバポートで有効になっており、コマンドが eth-storage 範囲で enable cdp を返す場合、Cisco Discovery Protocol はアプライアンスポートで有効になっています。**

```
ucs-fi# show configuration | egrep "^ scope|enable cdp"
.
.
.
 scope org
         enable cdp
.
.
.
 scope eth-storage
         enable cdp
.
.
.
```

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リストされている製品だけがこの脆弱性の影響を受けることが知られています。

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 1000 シリーズ
- Firepower 2100 シリーズ
- Network Convergence System（NCS）520 シリーズ ルータ

シスコは、この脆弱性が Cisco IOS ソフトウェア、または Cisco IOS XE ソフトウェアには影響を与えないことも確認しました。

回避策

この脆弱性に対処する回避策はありません。

ただし、Cisco Discovery Protocol の機能を使用しないお客様は、このプロトコルをグローバルに無効にして攻撃ベクトルを完全に閉じるか、各インターフェイスで無効にして攻撃対象領域を縮小できます。

Cisco FXOS ソフトウェアで Cisco Discovery Protocol を無効にする

Cisco Discovery Protocol は常に有効化され、Cisco FXOS ソフトウェアでは無効にできません。

Cisco FXOS ソフトウェアリリース2.1 以降では、Cisco Discovery Protocol は管理（mgmt0）ポートでのみ有効化されています。

Cisco IOS XR ソフトウェアで Cisco Discovery Protocol をグローバルに無効にする

Cisco IOS XR ソフトウェアを実行しているデバイスで Cisco Discovery Protocol をグローバルに無効にするには、次の例に示すように、管理者はグローバル コンフィギュレーション モードで **no cdp コマンドを使用します。**

```
RP/0/RP0/CPU0:ios#conf t
Mon Dec  2 17:58:08.556 UTC
RP/0/RP0/CPU0:ios(config)#no cdp
RP/0/RP0/CPU0:ios(config)#exit
Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:yes
```

Cisco IOS XR ソフトウェアのインターフェイスで Cisco Discovery Protocol を無効にする

Cisco IOS XR ソフトウェアを実行している特定デバイスの特定のインターフェイスで Cisco Discovery Protocol を無効にするには、次の例に示すように、管理者はインターフェイス コンフィギュレーション モードで **no cdp コマンドを使用します。**

```
RP/0/RP0/CPU0:ios#conf t
Mon Dec  2 18:00:08.622 UTC
RP/0/RP0/CPU0:ios(config)#interface GigabitEthernet0/0/0/0
RP/0/RP0/CPU0:ios(config-if)#no cdp
RP/0/RP0/CPU0:ios(config-if)#end
Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:yes
```

Cisco NX-OS ソフトウェアを実行している Cisco Nexus スイッチで Cisco Discovery Protocol をグローバルに無効にする

Cisco NX-OS ソフトウェアを実行している Cisco Nexus スイッチで Cisco Discovery Protocol をグローバルに無効にするには、次の例に示すように、管理者はグローバル コンフィギュレーション モードで no cdp enable コマンドを使用します。

```
nxos# conf t
Enter configuration commands, one per line. End with CNTL/Z.
nxos(config)# no cdp enable
nxos(config)# end
nxos# copy running-config startup-config
[########################################] 100%
Copy complete.
```

Cisco NX-OS ソフトウェアを実行している Cisco Nexus スイッチのインターフェイスで Cisco Discovery Protocol を無効にする

Cisco NX-OS ソフトウェアを実行している Cisco Nexus スイッチのインターフェイスで Cisco Discovery Protocol を無効にするには、次の例に示すように、管理者はインターフェイス コンフィギュレーション モードで no cdp enable コマンドを使用します。

```
nxos# conf t
Enter configuration commands, one per line. End with CNTL/Z.
nxos(config)# interface Ethernet1/1
nxos(config-if)# no cdp enable
nxos(config-if)# end
nxos# copy running-config startup-config
[########################################] 100%
Copy complete.
```

Cisco UCS ファブリック インターコネクトで Cisco Discovery Protocol を無効にする

Cisco UCS ファブリック インターコネクトで Cisco Discovery Protocol を完全に無効にすることはできません。

Cisco Discovery Protocol は、Cisco UCS ファブリック インターコネクトのサーバポートとアプライアンスポートで無効にできますが、イーサネット アップリンク ポート、イーサネット ポート チャネル メンバー、FCoE アップリンクポート、または管理ポートでは無効にできません。

Cisco UCS ファブリック インターコネクトのサーバポートで Cisco Discovery Protocol を無効にするには、次の例に示すように、管理者は **org 範囲のデフォルトの nw-ctrl-policy で disable cdp コマンドを使用します。**

```
ucs-fi# scope org
ucs-fi /org # enter nw-ctrl-policy default
ucs-fi /org/nw-ctrl-policy # disable cdp
ucs-fi /org/nw-ctrl-policy* # exit
ucs-fi /org* # exit
ucs-fi* # commit-buffer
ucs-fi#
```

Cisco UCS ファブリック インターコネクトのアプライアンスポートで Cisco Discovery Protocol を無効にするには、次の例に示すように、管理者は **eth-storage 範囲のデフォルトの nw-ctrl-policy で disable cdp コマンドを使用します。**

```
ucs-fi* # scope eth-storage
ucs-fi /eth-storage* # enter nw-ctrl-policy default
ucs-fi /eth-storage/nw-ctrl-policy* # disable cdp
ucs-fi /eth-storage/nw-ctrl-policy* # exit
ucs-fi /eth-storage* # exit
ucs-fi* # commit-buffer
ucs-fi#
```

修正済みソフトウェア

シスコでは、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、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、シスコから直接、あるいはシスコ認定リセラーまたはパートナーからそのソフトウェアの有効なライセンスを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

次の表では、左の列にシスコ ソフトウェアのリリースを記載しています。右側の列は、リリースがこのアドバイザリに記載されている脆弱性の影響を受けているかどうか、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。

Firepower 4100 シリーズおよび Firepower 9300 セキュリティ アプライアンスCSCvr15083

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

2.2 より前	修正済みリリースに移行
2.2	修正済みリリースに移行
2.3	2.3.1.173
2.4	リリース番号未定（2020 年 5 月）
2.6	2.6.1.187
2.7	2.7.1.106

注：Cisco FXOS ソフトウェアリリース 2.1 以降では、この脆弱性は管理（mgmt0）ポートを介してのみエクスプロイト可能です。これらのリリースでは、Cisco Discovery Protocol は、設定されていたとしても、実際には前面パネルポートで有効になりません。

IOS XR ソフトウェア：CSCvr15024

Cisco IOS XR 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
6.6 より前	適切な SMU
6.61	6.6.3 または適切な SMU
7.0	7.0.2（2020 年 3 月）または適切な SMU
7.1	脆弱性なし

1.ホワイトボックスルータでCisco IOS XRソフトウェアリリース6.6を実行しているお客様には、リリース6.6.12にアップグレードしてから、ソフトウェアメンテナンスアップグレード(SMU)をインストールすることを推奨します。 他のプラットフォームで Cisco IOS XR ソフトウェアリリース 6.6 を実行しているお客様は、Cisco IOS XR ソフトウェアリリース 6.6.3 にアップグレードすることをお勧めします。

Cisco IOS XR ソフトウェアでは、次の SMU も使用できます。

Cisco IOS XR ソフトウェア リリース	プラットフォーム	SMU 名
5.2.5	NCS6K	ncs6k-5.2.5.CSCvr78185
6.4.2	ASR9K-PX	asr9k-px-6.4.2.CSCvr78185
	CRS-PX	hfr-px-6.4.2.CSCvr78185
6.5.3	ASR9K-PX	asr9k-px-6.5.3.CSCvr78185
	ASR9K-X64	asr9k-x64-6.5.3.CSCvr78185
	NCS540	ncs540-6.5.3.CSCvr78185
	NCS560	ncs560-6.6.25.CSCvr78185
	NCS5K	ncs5k-6.5.3.CSCvr78185
	NCS5500	ncs5500-6.5.3.CSCvr78185
	XRV9K	xrv9k-6.5.3.CSCvr78185
6.6.12	ホワイトボックス	iosxrwbd-6.6.12.CSCvr78185
6.6.25	NCS560	ncs560-6.6.25.CSCvr78185
7.0.1	NCS540L	ncs540l-7.0.1.CSCvr78185

Cisco IOS XR ソフトウェアにおける SMU のダウンロード場所とインストール方法の詳細については、『IOS XR Software Maintenance Updates (SMUs)』ガイドを参照してください。

MDS 9000 シリーズ マルチレイヤ スイッチ：CSCvr15073

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(29)
6.2	6.2(29)
7.3	8.4(1a)
8.1	8.4(1a)
8.2	8.4(1a)
8.3	8.4(1a)
8.4	8.4(1a)

VMware vSphere 向け Nexus 1000 Virtual EdgeCSCvr15078

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	5.2(1)SV5(1.3)

Microsoft Hyper-V 向け Nexus 1000V スイッチ：CSCvr15078

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 より前	修正なし[1]
5.2	修正なし[1]

1. Cisco Nexus 1000V Switch for Microsoft Hyper-Vは、ソフトウェアメンテナンスが終了しています。

VMware vSphere 向け Nexus 1000V スイッチ：CSCvr15078

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 より前	5.2 (1) SV3 (4.1 b)
5.2	5.2 (1) SV3 (4.1 b)

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：CSCvr14976

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)I より前	7.0(3)I7(8)（2020年2月）または適切なSMU[1]
7.0(3)I	7.0(3)I7(8)（2020年2月）または適切なSMU[1]
7.0(3)F2	9.3(2)
9.2	9.3(2)
9.3	9.3(2)

1. Cisco NX-OSソフトウェアリリース7.0(3)I7(5a)、7.0(3)I7(6)、および7.0(3)I7(7)で利用可能なSMUにより、この脆弱性が修正されました(CSCvr14976)。 また、アドバイザリ「 Cisco NX-OS ソフトウェアの Cisco Discovery Protocol におけるリモートコード実行の脆弱性（Cisco NX-OS Software Cisco Discovery Protocol Remote Code Execution Vulnerability）」に記載されている脆弱性（CSCvr09175）も修正されます。SMU のファイル名は次の形式になります。 *CSCvr09175-n9k_ALL-1.0.0-<NX-OS_Release>.lib32_n9000.rpm*。

2. Cisco NX-OSソフトウェア7.0(3)Fトレインは、Cisco Nexus 3600プラットフォームスイッチおよびCisco Nexus 9500 Rシリーズスイッチングプラットフォームでのみ動作し、メンテナンスが終了しています。お客様は、Cisco NX-OS ソフトウェアリリース 9.2 以降に移行することをお勧めします。

SMU のインストール手順

Cisco.com の Software Center から SMU をダウンロードするには、次の手順を実行します。

1. [すべてを参照（Browse All）] をクリックします。
2. [IOSおよびNX-OSソフトウェア（IOS and NX-OS Software）] > [NX-OS] > [NX-OSソフトウェア（NX-OS Software）] > [スイッチ（Switches）] > [データセンタースイッチ（Data Center Switches）] の順に選択します。
3. 該当する製品とモデルを選択します。
4. [NX-OSソフトウェアメンテナンスアップグレード（SMU）（NX-OS Software Maintenance Upgrades (SMU)）] を選択します。
5. 適切な製品ページの左ペインからリリースを選択します。

注：SMU のファイル名は次の形式になります。*CSCvr09175-n9k_ALL-1.0.0-<NX-OS_Release>.lib32_n9000.rpm*。たとえば、Cisco NX-OSソフトウェアリリース7.0(3)I7(6)のSMUファイル名は*CSCvr09175-n9k_ALL-1.0.0-7.0.3.I7.6.lib32_n9000.rpm*です。

適切な SMU をインストールするには、SMU を*ブートフラッシュ：*スイッチのファイルシステムにコピーし、修正（ホットパッチ）をアクティブ化する次のコマンドを実行します。

1. **install add bootflash:<SMU_filename> activate**
2. **install commit**

次の例は、Cisco NX-OS ソフトウェアリリース 7.0(3)I7(6) 用の SMU をインストールするためのコマンドを示しています。

```
nx-os# install add bootflash:CSCvr09175-n9k_ALL-1.0.0-7.0.3.I7.6.lib32_n9000.rpm activate
nx-os# install commit
```

注：これらの手順は、この特定の種類の SMU のみに適用されます。

Nexus 5500/5600 プラットフォーム スイッチおよび Nexus 6000 シリーズ スイッチ：CSCvr15079

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
7.1 より前	7.3(6)N1(1)
7.1	7.3(6)N1(1)
7.3	7.3(6)N1(1)

Nexus 7000 シリーズ スイッチ：CSCvr15073

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 (24)
6.2	6.2 (24)
7.2	7.3(5)D1(1)
7.3	7.3(5)D1(1)
8.0	8.2(5)
8.1	8.2(5)
8.2	8.2(5)
8.3	8.4(2)（2020年3月）または適切なSMU[1]
8.4	8.4(2)（2020年3月）または適切なSMU[1]

1. Cisco NX-OSソフトウェアリリース8.4(1)では、次のSMUを使用できます。n7000-s2-dk9.8.4.1.CSCvs27997.bin、n7700-s2-dk9.8.4.1.CSCvs27997.bin、および n7700-s3-dk9.8.4.1.CSCvs27997.bin。Cisco NX-OS ソフトウェアリリース 8.3 を実行しているお客様は、Cisco NX-OS ソフトウェアリリース 8.4(1) にアップグレードしてから適切な SMU を適用することをお勧めします。

Cisco Nexus 7000 シリーズ スイッチ向け Cisco NX-OS ソフトウェアにおける SMU のダウンロード場所とインストール方法の詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』の「Performing Software Maintenance Upgrades」の章を参照してください。

ACIモードのNexus 9000シリーズファブリックスイッチ：CSCvr15072

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
13.1 より前	13.2(9b)
13.1	13.2(9b)
13.2	13.2(9b)
14.0	14.2(1j)
14.1	14.2(1j)
14.2	14.2(1j)

UCS 6200、6300、および 6400 シリーズ ファブリック インターコネクト：CSCvr15082 および CSCvr15111

Cisco UCS 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
3.2 より前	3.2(3n)
3.2	3.2(3n)
4.0	4.0 (4g)

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判別については、次の推奨リリースの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後のリリースを推奨す

る場合は、アドバイザリ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 Series Switches
Cisco Nexus 5500 プラットフォーム スイッチ
Cisco Nexus 5600 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 に最適なリリースを確認するには、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、このアドバイザリに記載されている脆弱性の公表を確認していません。この脆弱性の悪用に関する情報は Cisco PSIRT に寄せられていません。

出典

この脆弱性を報告していただいた Armis 社の Barak Hadad 氏に感謝いたします。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-fxnxos-iosxr-cdp-dos

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.3	使用可能な最初の修正済みリリースの表を更新。	修正済みソフトウェア	Interim	2020年2月21日

1.2	存在しない FXOS 2.5 を削除。脆弱性のある製品および回避策を反映して FXOS CDP 情報を更新。	「脆弱性のある製品」、「回避策」、「修正済みソフトウェア」	Interim	2020年2月7日
1.1	Cisco FXOS および Cisco UCS ファブリック インターコネクトが脆弱になるタイミング、Cisco FXOS および Cisco UCS ファブリック インターコネクトの移行オプション、Cisco FXOS および Cisco Nexus 1000 Virtual Edge for VMware vSphere の脆弱性のあるリリースと最初の修正済みリリースに関する情報を修正しました。	「脆弱性のある製品」、「回避策」、「修正済みソフトウェア」	Interim	2020年2月6日
1.0	初回公開リリース	—	Interim	2020年2月5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。