Cisco FXOSおよびNX-OSソフトウェアのCisco Discovery Protocolサービスにおける DoS脆弱性

Medium	**アドバイザリーID :** cisco-sa-cdp-dos-G8DPLWYG **初公開日 :** 2022-02-23 16:00 **最終更新日 :** 2022-03-01 17:35 **バージョン 1.1 :** Final **CVSSスコア :** 4.3 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvz72442 CSCvz72464 CSCvz72465 CSCvz74433 CSCvz72466 CSCvz72467 CSCvz72462 CSCvz72463	CVE-2022-20625

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Cisco Discovery Protocol(CDP)サービスの脆弱性により、認証されていない隣接する攻撃者がサービスを再起動させ、サービス拒否(DoS)状態を引き起こす可能性があります。

この脆弱性は、Cisco Discovery Protocolサービスによって処理されるCisco Discovery Protocolメッセージの不適切な処理に起因します。攻撃者は、一連の悪意のあるCisco Discovery Protocol(CDP)メッセージを該当デバイスに送信することで、この脆弱性を不正利用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Cisco Discovery Protocolサービスに障害を発生させ、再起動する可能性があります。まれに、プロセスの障害が繰り返し発生し、デバイス全体が再起動する可能性があります。

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cdp-dos-G8DPLWYG

このアドバイザリは、2022年2月のCisco FXOSおよびNX-OSソフトウェアセキュリティアドバイザリバンドル公開の一部です。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：2022年2月のCisco FXOSおよびNX-OSソフトウェアセキュリティアドバイザリバンドル公開。

該当製品

脆弱性のある製品

この脆弱性は、Cisco FXOS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次のシスコ製品に影響を与えました。

- Firepower 4100シリーズ(CSCvz72467)
- Firepower 9300セキュリティアプライアンス(CSCvz72467)
- MDS 9000シリーズマルチレイヤスイッチ(CSCvz72463)
- Nexus 1000 Virtual Edge for VMware vSphere(CSCvz72464)
- Microsoft Hyper-V向けNexus 1000Vスイッチ(CSCvz72464)
- VMware vSphere向けNexus 1000Vスイッチ(CSCvz72464)
- Nexus 3000シリーズスイッチ(CSCvz72442)
- Nexus 5500プラットフォームスイッチ(CSCvz72465)
- Nexus 5600プラットフォームスイッチ(CSCvz72465)
- Nexus 6000シリーズスイッチ(CSCvz72465)
- Nexus 7000シリーズスイッチ(CSCvz72463)
- 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)モードのNexus 9000シリーズファブリックスイッチ(CSCvz72462)
- スタンドアロンNX-OSモードのNexus 9000シリーズスイッチ(CSCvz72442)
- UCS 6200シリーズファブリックインターコネクト(CSCvz74433)
- UCS 6300シリーズファブリックインターコネクト(CSCvz74433)
- UCS 6400シリーズファブリックインターコネクト(CSCvz72466)

このアドバイザリの「修正済みソフトウェア」セクションを参照して、この公開時点で脆弱性が存在していたシスコソフトウェアリリースに関する情報を確認してください。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクション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。リリース2.1より前のCisco FXOSソフトウェアリリースでは、Cisco Discovery Protocolはすべてのフロントパネルポートで常に有効になっています。

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

デバイスで Cisco Discovery Protocol が有効になっているかを確認するには、**show running-config cdp all を実行します。 | 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（ネットワーク接続のために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、Fibre Channel over Ethernet(FCoE)アップリンクポート、および管理ポートで常に有効です。

Cisco Discovery Protocolは、サーバポート（Cisco UCS Managerドメイン内のサーバに提供されるインターフェイス）およびアプライアンスポート(直接接続されたネットワークファイルシステム(NFS)ストレージに接続するインターフェイス)でも有効にできます。 Cisco Discovery Protocolがデバイスのサーバポートまたはアプライアンスポートで有効になっているかどうかを確認するには、**show configuration | egrep "^ scope|enable cdp"コマンドを**使用します。コマンドが**org**スコープの下で**enable cdpコマンドを返す**と、Cisco Discovery Protocolはサーバポートで有効になります。コマンドが**eth**-storageスコープで**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ります。次の例は、サーバポートとアプライアンスポートでCisco Discovery Protocol(CDP)が有効になっているデバイスの出力を示しています。

```
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Cisco Firepower 1000シリーズおよびCisco Firepower 2100シリーズには影響を与えないことを確認しました。

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)ポートでのみ有効になっています。

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、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、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 CS 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、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、**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、**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#
```

これらの緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

修正済みソフトウェア

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 セキュリティ アドバイザリ 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アップグレード ソリューション一式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。

Cisco FXOS ソフトウェア

発行時点では、次の表のリリース情報が正確でした。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

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

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	修正済みリリースに移行。
2.3	2.3.1.219
2.4	修正済みリリースに移行。
2.5	修正済みリリースに移行。
2.6	修正済みリリースに移行。
2.7	修正済みリリースに移行。
2.8	修正済みリリースに移行。
2.9	2.9.1.158
2.10	2.10.1.179
2.11	脆弱性なし

Cisco NX-OS ソフトウェア

お客様が Cisco NX-OS ソフトウェアの脆弱性による侵害の可能性を判断できるよう、シスコでは Cisco Software Checker を提供しています。このツールにより、特定の Cisco NX-OS ソフトウェアリリースに該当するシスコ セキュリティアドバイザリ、および各アドバイザリで説明されている脆弱性が修正された最初のリリース（「First Fixed」）を特定できます。 また該当する場合、そのリリースに関するすべてのアドバイザリの脆弱性が修正された最初のリリース（「Combined First Fixed」）を特定できます。

お客様は、Cisco Software Checker を使用して次の方法でアドバイザリを検索できます。

- ソフトウェア、プラットフォーム、および 1 つ以上のリリースを選択する
- 特定のリリースのリストを含む .txt ファイルをアップロードする
- **show version コマンドの出力を入力する**

検索を開始した後で、すべてのシスコ セキュリティ アドバイザリまたは 1 つ以上の特定のアド

バイザリが含まれるように検索をカスタマイズできます。

また、次のフォームを使用して、Cisco NX-OS ソフトウェアとプラットフォームを選択、およびリリースを入力することで（例：Cisco Nexus 3000 シリーズ スイッチの **7.0(3)I7(5)**、**ACI モードの Cisco NX-OS ソフトウェアの 14.0(1h)**）、**シスコ セキュリティ アドバイザリの対象となるリリースであるかを判断することもできます。**

デフォルトでは、Cisco Software Checker の結果には、Security Impact Rating（SIR）が「重大」または「高」の脆弱性だけが含まれます。「中間」の SIR 脆弱性の結果を含めるには、Cisco Software Checker を使用して、検索をカスタマイズするときに [影響の評価（Impact Rating）] **ドロップダウンリストの [中間（Medium）]** チェックボックスをオンにします。

Cisco Nexus 3000、7000、および9000シリーズスイッチSMU

シスコはこの脆弱性に対処する次の SMU もリリースしています。SMUは、Cisco.comのSoftware Centerからダウンロードできます。

Cisco NX-OS ソフトウェア リリース	Platform	SMU 名
7.0(3)I7(10)	Nexus 3000および9000シリーズスイッチ	nxos.CSCvz72442-n9k_ALL-1.0.0-7.0.3.I7.10.lib32_n9000.rpm
8.4(5)	Nexus 7000 シリーズ スイッチ	n7000-s2-dk9.8.4.5.CSCvz72463.bin n7700-s2-dk9.8.4.5.CSCvz72463.bin n7700-s3-dk9.8.4.5.CSCvz72463.bin
9.3(8)	Nexus 3000および9000シリーズスイッチ	nxos.CSCvz72442-n9k_ALL-1.0.0-9.3.8.lib32_n9000.rpm

これらのSMUのダウンロードとインストールの詳細については、Cisco Nexus 3000シリーズスイッチ、Cisco Nexus 7000シリーズスイッチ、またはCisco Nexus 9000シリーズスイッチのCisco NX-OSシステム管理設定ガイドの「ソフトウェアメンテナンスアップグレードの実実行」を」スイッチ。

Cisco UCS ソフトウェア

発行時点では、次の表のリリース情報が正確でした。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

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

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
4.0 より前	修正済みリリースに移行。

4.0	修正済みリリースに移行。
4.1	4.1(3h)
4.2	4.2(1l)[1]

1. UCSソフトウェアリリース4.2(1k)には、この脆弱性に対する修正も含まれています。ただし、リリース4.2(1k)は保留リリースです。

Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）は、このアドバイザリに記載されている該当するリリース情報と修正されたリリース情報のみを検証します。

その他のリソース

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際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 スイッチ向け Cisco Nexus 1000V
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 ソフトウェア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 PSIRT では、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は確認しておりません。

出典

シスコは、この脆弱性について報告してくださった Qihoo 360 社 CERT の Hou JingYi 氏に感謝いたします。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cdp-dos-G8DPLWYG

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	Nexus 9000シリーズファブリックスイッチに関する不具合情報を修正。	該当製品	最終版	2022年3月1日
1.0	初回公開リリース	—	最終版	2022年2月23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。