Cisco FXOS 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（DoS）および任意コード実行の脆弱性

アドバイザリーID : cisco-sa-nxos-cdp-dos-ce-wWvPucC9
CVE-2022-20824
初公開日 : 2022-08-24 16:00
バージョン 1.0 : Final
CVSSスコア : 8.8
回避策 : No workarounds available
Cisco バグ ID : CSCwb74497 CSCwb74496 CSCwb74495 CSCwb74494 CSCwb74493 CSCwb74513 CSCwb70210 CSCwb74498

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 ソフトウェアと Cisco NX-OS ソフトウェアの Cisco Discovery Protocol 機能の脆弱性により、認証されていない隣接した攻撃者が root 権限で任意のコードを実行したり、該当デバイスでサービス妨害（DoS）状態を引き起こしたりする可能性があります。

この脆弱性は、Cisco Discovery Protocol メッセージ内にある特定の値の不適切な入力検証に起因します。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 root 権限で任意のコードを実行したり、Cisco Discovery Protocol プロセスのクラッシュと再起動を繰り返して、該当デバイスのリロードを引き起こし、DoS 状態を発生させたりする危険性があります。

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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cdp-

dos-ce-wWvPucC9

このアドバイザリは、2022 年 8 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。アドバイザリとリンクの一覧については、『Cisco Event Response: August 2022 Semiannual Cisco FXOS and NX-OS Software Security Advisory Bundled Publication』を参照してください。

該当製品

脆弱性のある製品

次のシスコ製品で Cisco FXOS または NX-OS ソフトウェアの脆弱なリリースを実行しており、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いる場合、この脆弱性の影響を受けます。

- Firepower 4100 シリーズ (CSCwb74498)
- Firepower 9300 セキュリティアプライアンス (CSCwb74498)
- MDS 9000 シリーズ マルチレイヤ スイッチ (CSCwb74494)
- VMware vSphere 向け Nexus 1000 Virtual Edge (CSCwb74495)
- Microsoft Hyper-V 向け Nexus 1000V スイッチ (CSCwb74495)
- VMware vSphere 向け Nexus 1000V スイッチ (CSCwb74495)
- Nexus 3000 シリーズ スイッチ (CSCwb70210)
- Nexus 5500 プラットフォームスイッチ (CSCwb74496)
- Nexus 5600 プラットフォームスイッチ (CSCwb74496)
- Nexus 6000 シリーズ スイッチ (CSCwb74496)
- Nexus 7000 シリーズ スイッチ (CSCwb74494)
- ACI モードの Nexus 9000 シリーズ ファブリック スイッチ (CSCwb74493)
- スタンドアロン NX-OS モードの Nexus 9000 シリーズ スイッチ (CSCwb70210)
- UCS 6200 シリーズ ファブリック インターコネクト (CSCwb74497)
- UCS 6300 シリーズ ファブリック インターコネクト (CSCwb74497)
- UCS 6400 シリーズ ファブリック インターコネクト (CSCwb74513)

注：ACIモードのCisco Nexus 9000シリーズファブリックスイッチを除き、上記のリストのすべての製品でCisco Discovery Protocolがデフォルトで有効になっています。

脆弱性が存在する Cisco 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」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 FXOS ソフトウェアのすべてのリリースにおいて、Cisco Discovery Protocol は管理（mgmt0）ポートで常に有効化されています。リリース 2.1 より前の Cisco FXOS ソフトウェアリリースでは、管理（mgmt0）ポートに加えてすべての前面ポートでも、Cisco Discovery

Protocol は常に有効化されています。

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

Cisco NX-OS ソフトウェアを実行している Cisco MDS または Nexus スイッチで Cisco Discovery Protocol が有効になっているかを確認するには、デバイスの CLI で show running-config cdp all | include "cdp enable" コマンドを使用することにより、デバイスで Cisco Discovery Protocol が有効になっているかどうかを確認できます。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。

```
<#root>

nxos#

show running-config cdp all | include "cdp enable"

cdp enable
  cdp enable
```

さらに、show cdp all コマンドを使用して、デバイスに実装されたすべてのインターフェイスの Cisco Discovery Protocol ステータスを確認できます。

ACI モードの Cisco Nexus シリーズ ファブリック スイッチの Cisco Discovery Protocol ステータスを確認する

Cisco Discovery Protocol は、ACI モードの Cisco Nexus 9000 シリーズ ファブリック スイッチではデフォルトで無効になっています。デバイスのすべてのインターフェイスでCisco Discovery Protocol(CDP)のステータスを確認するには、デバイスのCLIでshow cdp allコマンドを使用します。 Cisco Discovery Protocolが少なくとも1つのインターフェイスで有効になっているかどうかを確認するには、show cdp all | grep "enabled on"コマンドを実行します。次の例のように、コマンドが何らかの出力を返す場合、Cisco Discovery Protocol は 1 つ以上のインターフェイスで有効になっています。

```
<#root>

nxos#

show cdp all | grep "enabled on"

    CDP enabled on interface
```

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 UCS 6200、6300、および 6400 シリーズ ファブリック インターコネクトでは、次のポートで Cisco Discovery Protocol が常に有効になっています。

- イーサネット アップリンク ポート（ネットワーク接続用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
- 管理ポート

Cisco Discovery Protocol は、サーバーポート（Cisco UCS Manager ドメインのサーバーに示されるインターフェイス）およびアプライアンスポート（アタッチされた NFS ストレージに直接接続するインターフェイス）でも有効になっている可能性があります。これらのポートの Cisco Discovery Protocol ステータスを確認するには、デバイスの CLI で show configuration | egrep "^ scope|enable cdp"コマンドをデバイスのCLIで実行します。コマンドが org 範囲の下に enable cdp を返した場合、Cisco Discovery Protocol はサーバーポートで有効になっています。コマンドが eth-storage 範囲の下に enable cdp を返した場合、Cisco Discovery Protocol はアプライアンスポートで有効になっています。次の例は、サーバーポートとアプライアンスポートで Cisco Discovery Protocol が有効になっているデバイスでコマンドを実行した場合の出力結果を示しています。

<#root>

```
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

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 を使用しないい場合は、この機能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、個々の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 NX-OS ソフトウェアを実行している Cisco MDS および Nexus スイッチで Cisco Discovery Protocol をグローバルに無効にする

Cisco MDS または 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。

<#root>

```
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 MDS および 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 MDS または 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。

<#root>

```
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ー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、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。

<#root>

```
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。

<#root>

```
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

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リリースしています。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

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、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。

Cisco.com の Cisco Support and Downloads ページには、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス (My Devices)] ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。

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。

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（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

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。

Cisco FXOS および NX-OS ソフトウェア

お客様が Cisco FXOS および 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に、シスコは Cisco Software Checker を提供しています。このツールを使うことで、特定のソフトウェアリリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース（「First Fixed」）を特定できます。また、該当する場合には、Software Checker により判別されたすべてのアドバイザリに記載のすべて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。

このツールを使用するには、「Cisco Software Checker」ページの手順に従います。または、次のフォームを使用して、特定のソフトウェアリリースに影響を及ぼす脆弱性を検索します。このフォームを使用するには、次の手順に従います。

1. ツールで検索するアドバイザリを選択します。このアドバイザリのみ、セキュリティ影響評価（SIR）が「重大」または「高」のアドバイザリのみ、すべてのアドバイザリのいずれかです。
2. 該当するソフトウェアを選択します。
3. 該当するプラットフォームを選択します。
4. リリース番号を入力します。たとえば、Cisco Firepower 4100 シリーズ セキュリティ アプライアンスの場合は 2.9.1.158、Cisco Nexus 3000 シリーズ スイッチの場合は 7.0(3)I7(5) です。
5. [チェック（Check）] をクリックします。

2		Critical,High,Medium
このアドバイザのみ	Cisco FXOS ソフトウェア	
あらゆるプラットフォーム		

Enter Version | Check

Cisco Nexus 3000、7000、および 9000 シリーズ スイッチの 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。次の SMU を 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
8.2(8)	Nexus 7000 シリーズ スイッチ	n7000-s2-dk9.8.2.8.CSCwc36631.bin n7700-s2-dk9.8.2.8.CSCwc36631.bin
9.3(9)	Nexus 3000 および 9000 シリーズ スイッチ	nxos.CSCwb70210-n9k_ALL-1.0.0-9.3.9.lib32_n9000.rpm

Cisco Nexus 3000、7000、9000 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、およびCisco Nexus 9000 シリーズ スイッチの『Cisco NX-OS System Management Configuration Guide』の「Performing Software Maintenance Upgrades」セクションを参照してください。

Cisco UCS ソフトウェア

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。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。右側の列は、リリースがこのバンドルに記載された「重大」および「高」影響の脆弱性のいずれかに該当するかどうか、およびそれらの脆弱性に対する修正を含むリリースを示しています。

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	アドバイザリのバンドルに記載されているすべての脆弱性に対する最初の修正済みリリース
4.1 より前	修正済みリリースに移行。	修正済みリリースに移行。
4.1	4.1(3i)	4.1(3i)
4.2	4.2(1n)	4.2(1n)

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。

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

この脆弱性を報告していただいた、オランダ国家サイバー セキュリティ センターに勤務する匿名の研究者に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cdp-dos-ce-wWvPucC9

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2022 年 8 月 24 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。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。