

Cisco NX-OS ソフトウェアの Cisco Fabric Services over IP におけるサービス妨害に関する脆弱性

High アドバイザリーID : cisco-sa-cfsoip-dos-tpykyDr [CVE-2022-20624](#)
初公開日 : 2022-02-23 16:00
バージョン 1.0 : Final
CVSSスコア : [8.6](#)
回避策 : No workarounds available
Cisco バグ ID : [CSCvy95696](#)
[CSCvy95840](#)

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 NX-OSソフトウェアのCisco Fabric Services over IP(CFSolP)機能の脆弱性により、認証されていないリモートの攻撃者が該当デバイスでサービス拒否(DoS)状態を引き起こす可能性があります。

この脆弱性は、着信CFSolPパケットの不十分な検証に起因します。攻撃者は、巧妙に細工されたCFSolPパケットを該当デバイスに送信することにより、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者は該当デバイスのリロードを引き起こし、その結果 DoS 状態が発生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-cfsoip-dos-tpykyDr>

このアドバイザリーは、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ーバンドル公開の一部です。これらのアドバイザリー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ーバンドル公開。](#)

該当製品

脆弱性のある製品

この脆弱性は、Cisco NX-OSソフトウェアの脆弱性のあるリリースを実行し、CFSolP機能を有効にしている次のシスコ製品に影響を与えます。

- Nexus 3000シリーズスイッチ([CSCvy95696](#))
- スタンドアロンNX-OSモードのNexus 9000シリーズスイッチ([CSCvy95696](#))
- UCS 6400シリーズファブリックインターコネクタ([CSCvy95840](#))

注：Nexus 3000およびNexus 9000シリーズスイッチでは、CFSolPはデフォルトでは有効になっていません。UCS 6400シリーズファブリックインターコネクタでは、CFSolPがデフォルトで有効になっています。

CFSolPが有効になっているかどうかの確認

CFSolPが有効になっているかどうかを確認するには、Cisco NX-OSのCLIで**show cfs status**コマンドを使用し、**Distribution over IP**のステータスを確認します。**Distribution over IP**が**Enabled**の場合、次の例のようにCFSolPが有効になります。

```
switch# show cfs status
Distribution : Enabled
Distribution over IP : Enabled
IPv4 multicast address : 239.255.70.83
IPv6 multicast address : ff15::efff:4653
Distribution over Ethernet : Disabled
```

注：Cisco UCSファブリックインターコネクタでは、まず**connect nxos**コマンドを使用してCisco NX-OS CLIを入力し、次に**show cfs status**コマンドを使用します。

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
- 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
- VMware vSphere 向け Nexus 1000 Virtual Edge
- Nexus 1000V Switch for Microsoft Hyper-V

- Nexus 1000V Switch for VMware vSphere
- 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)
- 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

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ン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。

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 Cisco Service Contract 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 POS 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、本アドバイザーの URL をご用意ください。

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ー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ー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ーを検索できます。

- 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ー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 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.CSCvy95696-n9k_ALL-1.0.0-7.0.3.I7.10.lib32_n9000.rpm |
| 9.3(8) | Nexus 3000および9000シリーズスイッチ | CSCvy95696-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行」セクション](#)を参照してください。

Cisco UCS ソフトウェア

次の表に示すように、該当する修正済みのソフトウェアリリースにアップグレードすることをお勧めします。

UCS 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 | 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

この脆弱性を報告していただいたNational Security Agency(NSA)に感謝いたします。

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cfsoip-dos-tpykyDr>

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 | — | 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。