Cisco NX-OS ソフトウェアの Cisco Fabric Services 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-20190306-nxos-fabric-dos

初公開日 : 2019-03-06 16:00

最終更新日 : 2019-03-19 20:55

バージョン 1.1 : Final

CVSSスコア : 8.6

回避策 : No workarounds available

Cisco バグ ID : CSCvj10181 CSCvh99066 CSCvj10183 CSCvj10176 CSCvj10178

CVE-2019-1616

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 コンポーネントにおける脆弱性により、認証されていないリモート攻撃者が、バッファ オーバーフローを引き起こせるようになり、サービス妨害（DoS）状態になる可能性があります。

この脆弱性は、Cisco Fabric Services パケットが十分に検証されていないことに起因しています。 細工された Cisco Fabric Services のパケットが該当デバイスに送信されると、本脆弱性がエクスプロイトされる危険性があります。 エクスプロイトに成功すると、攻撃者は、デバイスでバッファ オーバーフロー状態を引き起こせるようになり、プロセスがクラッシュして 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-20190306-nxos-fabric-dos

このアドバイザリは、2019 年 3 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。このバンドルの中には、26 件の脆弱性に関する 25 件のシスコ セキュリティ アドバイザリが含まれています。 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： 2019 年 3 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。

該当製品

脆弱性のある製品

本脆弱性は、Cisco NX-OS ソフトウェアの脆弱性のあるリリースを実行する次のシスコ製品に影響を与えます。

- 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 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 ラインカードおよびファブリック モジュール
- 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 Fabric Services を使用するようにデバイスが設定されているかどうかを判断する方法については、このアドバイザリの「詳細」の項を参照してください。

脆弱性が存在する Cisco 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。

Cisco NX-OS ソフトウェア リリースの判別

管理者は、デバイスの CLI で **show version コマンド**を使用することによって、デバイスで実行されている Cisco NX-OS ソフトウェアのリリースをチェックできます。 デバイスが Cisco NX-OS ソフトウェア リリース **7.0(3)I5(1)** を実行している場合、コマンドの出力例は次のようになります。

```
nxos-switch# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2016, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source.  This software is provided "as is," and
unless otherwise stated, there is no warranty, express or implied,
including but not limited to warranties of merchantability and fitness
for a particular purpose. Certain components of this software are
licensed under the GNU General Public License (GPL) version 2.0 or
```

```
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
Software
  BIOS: version 07.57
  NXOS: version 7.0(3)I5(1) [build 7.0(3)I5(0.9)]
  BIOS compile time:  06/29/2016
  NXOS image file is: bootflash:///nxos.7.0.3.I5.0.9.bin
  NXOS compile time:  8/1/2016 23:00:00 [08/02/2016 00:30:32]
  .
  .
  .
```

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 ファイアウォール
- FirePOWER 4100 シリーズ次世代ファイアウォール製品
- Firepower 9300 セキュリティ アプライアンス
- Nexus 1000V Switch for Microsoft Hyper-V
- Nexus 1000V Switch for VMware vSphere
- Nexus 2000 シリーズ ファブリック エクステンダ
- 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 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）

詳細

Cisco Fabric Services は、同一ネットワーク上にあり仮想ポート チャネル（vPC）を使用するシスコ デバイス間で、設定データを配信・同期するための共通インフラストラクチャです。 Cisco Fabric Services との互換性があり、その使用が有効になっているアプリケーションおよび機能の設定データが含まれます。たとえば、分散型デバイス エイリアス サービス、Network Time Protocol（NTP）、ユーザと管理者のロールを挙げることができます。

データを配信および同期するために、Cisco Fabric Services は次の配信タイプのいずれかを使用するように設定できます。

- **Cisco Fabric Services over Fibre Channel（CFSoFC）：** 仮想ストレージ エリア ネットワーク（VSAN）などのファイバ チャネル（FC）でデータを配信します。 CFSoFC 配信はデフ

ォルトで有効になっています。

- **Cisco Fabric Services over Ethernet（CFSoE）：** イーサネット ネットワークでデータを配信します。 CFSoE のパケットは、vPC スイッチ ペア間で状態を同期するために使用される、vPC ピア リンクのみを通過します。 CFSoE 配信はデフォルトで無効になっています。
- **Cisco Fabric Services over IP（CFSoIP）：** IPv4 または IPv6 ネットワークでデータを配信します。 CFSoIP 配信はデフォルトで無効になっています。

このアドバイザリに記載された脆弱性は、該当ソフトウェアが、配信操作中および同期操作中に受信する Cisco Fabric Services のパケットを処理するときに不十分な入力検証が発生する可能性があることに起因しています。 脆弱性をエクスプロイトするために、何らかのアプリケーションが Cisco Fabric Services を使用できるようになっている必要はありません。 代わりに、エクスプロイトは、Cisco Fabric Services のどの配信タイプがデバイスに対して設定されているかに依存します。 さらに、どの配信タイプが設定されているかに基づいて、攻撃ベクトルは次のように異なります。

- **CFSoFC：** デバイスで FC ポートが設定されている場合は、Fibre Channel over Ethernet（FCoE）または Fibre Channel over IP（FCIP）経由で攻撃が発生する可能性があります。 このシナリオでは、攻撃は、管理プレーンではなく、いずれかの FC ポートのデータ プレーンで成功する可能性があります。 デバイスの FC ポートが設定されていない場合、この配信タイプを使用して脆弱性をエクスプロイトすることはできません。
- **CFSoE：** vPC ピア リンクに直接アクセスできる攻撃者から攻撃を受ける可能性があります。 その他のピア、ネイバー、または vPC 接続デバイスを使用して脆弱性をエクスプロイトすることはできません。
- **CFSoIP：** デバイスの管理インターフェイスに IP ネットワーク接続するすべてのノードから攻撃を受ける可能性があります。 このシナリオでは、データ プレーンからの攻撃が成功する可能性はありません。

デバイスで複数の配信タイプの使用が有効になっている場合は、デバイスに対して、それらすべての配信タイプに適用可能な攻撃ベクトルが存在します。

管理者は、次の例に示すように、デバイスの CLI で **show cfs status コマンド**を使用して、設定情報を表示し、デバイスの Cisco Fabric Services の配信ステータスをチェックできます。

```
switch# show cfs status

Distribution : Enabled
Distribution over IP : Disabled
IPv4 multicast address : 239.255.70.83
IPv6 multicast address : ff15::efff:4653
Distribution over Ethernet : Disabled
```

前に示した例では、コマンド出力の **Distribution** フィールドの値が *Enabled* であることが、デバイスで Cisco Fabric Services が有効になっていること、および Cisco Fabric Services のデフォルトの配信タイプ（CFSoFC）を使用するようにデバイスが設定されていることを示しています。 **Distribution over IP** フィールドと **Distribution over Ethernet** フィールドの値が *Disabled* であることが、CFSoIP および CFSoE の各配信タイプを使用するようにデバイスが追加設定されていないことを示しています。

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

この項の該当する表に示すように、適切なリリースにアップグレードすることをお勧めします。

完全なアップグレード ソリューションを確認するにあたっては、このアドバイザリが、公開されたバンドルの一部であることを考慮する必要があります。 バンドル アドバイザリの完全なリストは、次のページにあります。 シスコのイベント レスポンス： 2019 年 3 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。

次の表では、左の列に Cisco FXOS ソフトウェアまたは Cisco NX-OS ソフトウェアのリリースを示しています。 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。 右の列では、今回のアドバイザリ バンドルに記載された脆弱性全体に対する最初の修正リリースを、影響を受けるソフトウェア リリースごとに記載しています。

各表の右の列に記載されているリリースには、脆弱性に対する修正が含まれていますが、Cisco NX-OS ソフトウェア イメージの署名検証に関する脆弱性に関連する修正については、ソフトウェア アップグレードの一部として BIOS をアップグレードする必要があります。 以下に示すいずれかの製品のソフトウェアをアップグレードする場合は、このアドバイザリに記載されている BIOS アップグレードと、該当製品の ID および BIOS バージョンの詳細を参照することをお勧めします。

- Nexus 3000 シリーズ スイッチ
- ACI モードの Nexus 9000 シリーズ ファブリック 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 ラインカードおよびファブリック モジュール

MDS 9000 シリーズ マルチレイヤ スイッチ： CSCvj10178

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	アドバイザリ バンドルに記載されている脆弱性全体に対する最初の修正リリース
5.2	6.2(25)	6.2(27)
6.2	6.2(25)	6.2(27)
7.3	8.1(1b)	8.3(2)
8.1	8.1(1b)	8.3(2)
8.2	8.3(1)	8.3(2)
8.3	脆弱性なし	8.3(2)

Nexus 3000 シリーズ スイッチ： CSCvh99066

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	アドバイザリ バンドルに記載されている脆弱性全体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)I7(6)

7.0(3)I4	7.0(3)I4(9)	7.0(3)I7(6)
7.0(3)I5	7.0(3)I7(4)	7.0(3)I7(6)
7.0(3)I6	7.0(3)I7(4)	7.0(3)I7(6)
7.0(3)I7	7.0(3)I7(4)	7.0(3)I7(6)
9.2	脆弱性なし	9.2(2)

Nexus 3500 プラットフォーム スイッチ： CSCvj10181

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	アドバイザリ バンドルに記載されている脆弱性全体に対する最初の修正リリース
6.0(2)A8 より前	6.0(2)A8(10)	6.0(2)A8(11)
6.0(2)A8	6.0(2)A8(10)	6.0(2)A8(11)
7.0(3)	7.0(3)I7(4)	7.0(3)I7(6)
9.2	脆弱性なし	9.2(2)

Nexus 3600 プラットフォーム スイッチ： CSCvj10176

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	アドバイザリ バンドルに記載されている脆弱性全体に対する最初の修正リリース
7.0(3)F3	7.0(3)F3(3c)[1]	7.0(3)F3(5)
9.2	脆弱性なし	9.2(2)

[1]この脆弱性は、7.0(3)F3(4) では修正されていませんが、7.0(3)F3(5) で修正されています。

Nexus 7000 および 7700 シリーズ スイッチ CSCvj10178

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	アドバイザリ バンドルに記載されている脆弱性全体に対する最初の修正リリース
6.2 より前	脆弱性なし	6.2(22)
6.2	6.2(22)	6.2(22)
7.2	8.2(3)	8.2(3)
7.3	CSCvj10178 および CSCvj63807[1] のための Umbrella SMU	8.2(3)
8.0	8.2(3)	8.2(3)
8.1	8.2(3)	8.2(3)
8.2	8.2(3)	8.2(3)
8.3	脆弱性なし	8.3(2)

[1]ソフトウェア Nexus 7000 および 7700 を対象としたメンテナンス アップグレード（SMU）。 SMU ファイル名には、Cisco bug ID CSCvo56625 が含まれています。

スタンドアロン NX-OS モードの Nexus 9000 シリーズ スイッチ： CSCvh99066

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	アドバイザリ バンドルに記載されている脆弱性全体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)I7(6)
7.0(3)I4	7.0(3)I4(9)	7.0(3)I7(6)
7.0(3)I5	7.0(3)I7(4)	7.0(3)I7(6)
7.0(3)I6	7.0(3)I7(4)	7.0(3)I7(6)
7.0(3)I7	7.0(3)I7(4)	7.0(3)I7(6)
9.2	脆弱性なし	9.2(2)

Nexus 9500 R シリーズ ラインカードおよびファブリック モジュール： CSCvj10176

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	アドバイザリ バンドルに記載されている脆弱性全体に対する最初の修正リリース
7.0(3)F1	7.0(3)F3(3c)[1]	7.0(3)F3(5)
7.0(3)F2	7.0(3)F3(3c)[1]	7.0(3)F3(5)
7.0(3)F3	7.0(3)F3(3c)[1]	7.0(3)F3(5)
9.2	脆弱性なし	9.2(2)

[1]この脆弱性は、7.0(3)F3(4) では修正されていませんが、7.0(3)F3(5) で修正されています。

UCS 6200、6300、および 6400 ファブリック インターコネクト： CSCvj10183

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	アドバイザリ バンドルに記載されている脆弱性全体に対する最初の修正リリース
3.1 より前	3.2(3j)	3.2(3j)
3.1	3.2(3j)	3.2(3j)
3.2	3.2(3j)	3.2(3j)
4.0	4.0(2a)	4.0(2a)

関連情報

Cisco Nexus スイッチに最適な Cisco NX-OS ソフトウェア リリースの確認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 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-20190306-nxos-fabric-dos

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.1	Nexus 7000 および 7700 を対象として 7.3 ソフトウェア リリースの SMU 修正を追加。	修正済みソフトウェア	最終版	2019 年 3 月 19 日
1.0	初回公開リリース		最終版	2019 年 3 月 6 日

利用規約

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。