Cisco FXOS および NX-OS ソフトウェアの Cisco Fabric Services における任意のコード実行の脆弱性

Critical

アドバイザリーID : cisco-sa-20180620-fxnxos-fab-ace

初公開日 : 2018-06-20 16:00

最終更新日 : 2018-07-05 21:11

バージョン 1.1 : Final

CVSSスコア : 9.8

回避策 : No workarounds available

Cisco バグ ID : CSCve02463 CSCve02804 CSCvd69954 CSCve04859 CSCve02785 CSCve02787

CVE-2018-0308

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 Fabric Services コンポーネントの脆弱性により、認証されていないリモート攻撃者が任意のコードを実行したり、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。

本脆弱性は、Cisco Fabric Services のパケットのヘッダーの値が、該当ソフトウェアによって十分に検証され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。 エクスプロイトが成功すると、バッファ オーバーフローが発生し、任意のコードが実行されたり、DoS 状態が引き起こされたりする可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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-20180620-fxnxos-fab-ace

このアドバイザリは、2018 年 6 月に公開された Cisco FXOS および NX-OS ソフトウェアのセキ

ユリティ アドバイザリ コレクションの一部です。この中には、24 件の脆弱性に関する 24 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。Cisco Event Response: 2018 年 6 月 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 コレクション

該当製品

脆弱性のある製品

本脆弱性は、Cisco FXOS ソフトウェアまたは Cisco NX-OS ソフトウェアの脆弱性があるリリースを実行し、かつ Cisco Fabric Services を使用するように設定されている、次のシスコ製品に影響を与えます。

- 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
- MDS 9000 シリーズ マルチレイヤ スイッチ
- Nexus 2000 シリーズ ファブリック エクステンダ
- 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 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 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 6100 シリーズ ファブリック インターコネクト
- 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

脆弱性が存在する Cisco FXOS ソフトウェアおよび 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 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。

現在の Cisco FXOS ソフトウェア リリースを確認する

管理者は、デバイスの CLI で次のコマンドを使用するか、管理者用ポータルの [Overview] タブに移動して、デバイス上で実行されている Cisco FXOS ソフトウェアのリリースをチェックできます。 次に、Cisco FXOS ソフトウェア リリース 2.2(2.14) を実行しているデバイスでの **show version** CLI コマンドの出力例を示します。これは、コマンド出力の **Package-Vers** フィールドで確認できます。

```
QP4120B1 # scope system
QP4120B1 /system # show version
FPRM:
Running-Vers: 4.2(2.15)
Package-Vers: 2.2(2.14)
Activate-Status: Ready
```

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 7.3(2)D1(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
Documents: http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html
Copyright (c) 2002-2017, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
Software
  BIOS:      version 2.12.0
  kickstart: version 7.3(2)D1(1)
  system:    version 7.3(2)D1(1)
.
.
.
```

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 2100 シリーズ ファイアウォール
- Nexus 1000V シリーズ スイッチ
- Nexus 1100 シリーズ クラウド サービス プラットフォーム
- Nexus 3600 プラットフォーム 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)

Cisco では、本脆弱性が Cisco Nexus 4000 シリーズ スイッチ、Cisco Nexus 5010 スイッチ、Cisco Nexus 5020 スイッチに影響するかどうかを調査していません。これらの製品がサポート終了ステータスに達しているためです。 詳細については、「IBM BladeCenter 用の Cisco Nexus 4000 シリーズ スイッチ モジュールの販売終了およびサポート終了通知」および「Cisco Nexus 5010 および Nexus 5020 スイッチの販売終了およびサポート終了通知」を参照してください。

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）上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 ネットワーク上でデータを配信します。 vPC をサポートするには、この配信タイプを使用するように Cisco Fabric Services を設定する必要があります。 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 ネットワーク上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**：デバイスの 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、または vPC ピア リンクにアクセスできる攻撃者からのみ、攻撃の可能性があります。 その他のピア、ネイバー、ネットワーク ノード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

、攻撃の可能性があります。 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 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。このアドバイザリはコレクションの一部です。これらも考慮した上、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。 コレクションに含まれるアドバイザリとリンクの一覧については、次を参照してください。シスコのイベント対応： 2018 年 6 月 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 コレクション

次の表では、左の列に Cisco FXOS または 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。 右の列は、リリースがこのアドバイザリ集に記載された何らかの脆弱性に該当するかどうか、および、それらすべて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 シリーズ次世代ファイアウォール製品： CSCve04859

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	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories
1.1	1.1.4.179	2.0.1.159
2.0	2.0.1.153	2.0.1.159
2.1.1	2.1.1.86	2.1.1.86
2.2.1	2.2.1.70	2.2.2.17 または 2.3.1.58
2.2.2	2.2.2.17	2.2.2.17 または 2.3.1.58
2.3	脆弱性なし	脆弱性なし

Firepower 9300 セキュリティ アプライアンス： CSCve04859

Cisco FXOS ソフト	この脆弱性に対する最初の修正リ	First Fixed Release for All

ウェア リリース	リース	Vulnerabilities Described in the Collection of Advisories
1.1	1.1.4.179	2.0.1.159
2.0	2.0.1.153	2.0.1.159
2.1.1	2.1.1.86	2.1.1.86
2.2.1	2.2.1.70	2.2.2.17 または 2.3.1.58
2.2.2	2.2.2.17	2.2.2.17 または 2.3.1.58
2.3	脆弱性なし	脆弱性なし

MDS 9000 シリーズ マルチレイヤ スイッチ： CSCvd69954

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	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories
5.2	6.2(21)	8.1(1a) 8.2(1)
6.2	6.2(21)	8.1(1a) 8.2(1)
7.3	8.1(1a)	8.1(1a) 8.2(1)
8.1	8.1(1a)	8.1(1a) 8.2(1)
8.2	脆弱性なし	脆弱性なし

Nexus 3000 シリーズ スイッチ： CSCve02785

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	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories
7.0(3)I4 よりも前	7.0(3)I4(7)	7.0(3)I7(4)
7.0(3)I4	7.0(3)I4(7)	7.0(3)I7(4)
7.0(3)I5	7.0(3)I6(2)	7.0(3)I7(4)
7.0(3)I6	7.0(3)I6(2)	7.0(3)I7(4)
7.0(3)I7	脆弱性なし	7.0(3)I7(4)

Nexus 3500 プラットフォーム スイッチ： CSCve02785

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	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories
6.0	7.0(3)I7(2)	7.0(3)I7(4)
7.0.3	脆弱性なし	7.0(3)I7(4)

Nexus 2000、5500、5600、6000 シリーズ スイッチ： CSCve02463

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	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories

6.0	7.3(3)N1(1)	7.3(3)N1(1)
7.0	7.3(3)N1(1)	7.3(3)N1(1)
7.1	7.3(3)N1(1)	7.3(3)N1(1)
7.2	7.3(3)N1(1)	7.3(3)N1(1)
7.3	7.3(3)N1(1)	7.3(3)N1(1)

Nexus 7000 および 7700 シリーズ スイッチ CSCvd69954

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	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories
6.2	6.2(20)	8.1(2) または 8.2(1)
7.2	7.3(2)D1(1)	8.1(2) または 8.2(1)
7.3	7.3(2)D1(1)	8.1(2) または 8.2(1)
8.0	8.1(2)	8.1(2) または 8.2(1)
8.1	8.1(2)	8.1(2) または 8.2(1)
8.2	脆弱性なし	脆弱性なし

スタンドアロン NX-OS モードの Nexus 9000 シリーズ スイッチ： CSCve02785

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	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories
7.0(3)I4 よりも前	7.0(3)I4(7)	7.0(3)I7(4)
7.0(3)I4	7.0(3)I4(7)	7.0(3)I7(4)
7.0(3)I5	7.0(3)I6(2)	7.0(3)I7(4)
7.0(3)I6	7.0(3)I6(2)	7.0(3)I7(4)
7.0(3)I7	脆弱性なし	7.0(3)I7(4)

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： CSCve02804

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	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories
7.0	7.0(3)F3(1)	7.0(3)F3(3a)

UCS 6100、6200、6300 ファブリック インターコネクト CSCve02787

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	First Fixed Release for All Vulnerabilities Described in the Collection of Advisories
2.2 より前	3.2(2b)	3.2(2b)
2.2	3.2(2b)	3.2(2b)
2.5	3.2(2b)	3.2(2b)

3.0	3.2(2b)	3.2(2b)
3.1	3.2(2b)	3.2(2b)
3.2	3.2(2b)	3.2(2b)

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-20180620-fxnxos-fab-ace

改訂履歴

Version	Description	Section	Status	日付
1.1	FXOS MDS	修正済みソフトウェア	Final	2018 年 7 月 5 日
1.0	初回公開リリース		Final	2018 年 6 月 20 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。