Cisco NX-OS ソフトウェアの Internet Group Management Protocol のスヌーピングにおけるリモートのコード実行とサービス妨害の脆弱性

High

アドバイザリーID : cisco-sa-20180620-nxosigmp
初公開日 : 2018-06-20 16:00
最終更新日 : 2018-06-22 18:24
バージョン 1.1 : Final
CVSSスコア : 8.8
回避策 : No workarounds available
Cisco バグ ID : CSCuv79620 CSCvg71263

CVE-2018-0292

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 Internet Group Management Protocol（IGMP）のスヌーピング機能における脆弱性により、認証されていない隣接する攻撃者が任意のコードを実行し、該当システムのフル コントロールを取得する可能性があります。また、攻撃者は該当システム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。

本脆弱性は、IGMP スヌーピング サブシステムにおけるバッファ オーバーフロー状態に起因しています。細工された IGMP パケットが該当システムに送信されると、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、任意のコードが実行され、該当システムのフル コントロールを取得されるか、該当システムがリロードされ、DoS 状態が生じ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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180620-nxosigmp

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ュリティ 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。アドバイザリとリンクの一覧については、

『Cisco Event Response: June 2018 Cisco FXOS and NX-OS Software Security Advisory Collection』を参照してください。

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。

- Nexus 2000 シリーズ 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 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
- 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）
- スタンドアロン NX-OS モードの Nexus 9000 シリーズ スイッチ

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。

NX-OS ソフトウェアの脆弱性の確認

本脆弱性は、IGMP スヌーピング機能が設定された NX-OS デバイスにのみ影響を与えます。本脆弱性は、IP バージョン 4（IPv4）または IP バージョン 6（IPv6）のいずれかを経由して送信された IGMP スヌーピングに適用されます。

Nexus デバイスで IGMP スヌーピングが設定されているかどうかを確認するには、管理者が NX-OS CLI から show running-config | include "ip igmp snooping" コマンドを使用して、この機能が有効になっていることを確認します。コマンドの出力として ip igmp snooping が返された場合、デバイスに脆弱性が存在します。次の例は、NX-OS ソフトウェアを実行しているデバイスで IGMP スヌーピング機能が有効になっていることを示しています。
<#root>

```
nxos-switch#
show running-config | include "ip igmp snooping"
ip igmp snooping
```

注：特定のNX-OSハードウェアプラットフォームでは、IGMPスヌーピングはデフォルトで有効になっており、実行コンフィギュレーションに明示的に表示されません。https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3000/sw/multicast/503_u5_1/multicas 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 7.3(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。

<#root>

```
nxos-switch#
```

show version

<#root>

```
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
- Firepower 4100 シリーズ次世代ファイアウォール
- 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 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 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

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。

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。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 http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載の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。

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、[シスコのセキュリティアドバイザリおよびアラート（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(http://www.cisco.com/en/US/support/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。

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。アドバイザリとリンクの一覧については、『Cisco Event Response: June 2018 Cisco FXOS and NX-OS Software Security Advisory Collection』を参照してください。

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。

Nexus 3000シリーズスイッチ：CSCuv79620

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(1)	7.0(3)I7(4)
7.0(3)I4	7.0(3)I4(1)	7.0(3)I7(4)
7.0(3)I5	7.0(3)I7(1)	7.0(3)I7(4)
7.0(3)I6	7.0(3)I7(1)	7.0(3)I7(4)
7.0(3)I7	7.0(3)I7(1)	7.0(3)I7(4)

Nexus 3500プラットフォームスイッチ：CSCuv79620

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(2)	7.0(3)I7(2)	7.0(3)I7(4)
7.0(3)	7.0(3)I7(2)	7.0(3)I7(4)

Nexus 2000、5500、5600、および6000シリーズスイッチ：CSCuv79620

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：CSCuv79620

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	8.1(2)	8.1(2) または 8.2(1)
7.2	8.1(2)	8.1(2) または 8.2(1)
7.3	8.1(2)	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

ACI モードの Nexus 9000 シリーズ ファブリック スイッチ： CSCvg71263

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
12.1/2.1 よりも前	13.1(1i)/3.1(1i)	13.1(1i)/3.1(1i)
12.1/2.1	13.1(1i)/3.1(1i)	13.1(1i)/3.1(1i)
12.2/2.2	13.1(1i)/3.1(1i)	13.1(1i)/3.1(1i)
12.3/2.3	13.1(1i)/3.1(1i)	13.1(1i)/3.1(1i)
13.0/3.0	13.1(1i)/3.1(1i)	13.1(1i)/3.1(1i)

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
13.1/3.1	13.1(1i)/3.1(1i)	13.1(1i)/3.1(1i)

スタンドアロンNX-OSモードのNexus 9000シリーズスイッチ：CSCuv79620

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(1)	7.0(3)I7(4)
7.0(3)I4	7.0(3)I4(1)	7.0(3)I7(4)
7.0(3)I5	7.0(3)I7(1)	7.0(3)I7(4)
7.0(3)I6	7.0(3)I7(1)	7.0(3)I7(4)
7.0(3)I7	7.0(3)I7(1)	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と Nexus 3600プラットフォームスイッチ：CSCuv79620

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(3)	7.0(3)F3(3a)

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180620-nxosigmp

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	内部バージョンのマッピング情報を更新	N/A	Final	2018 年 6 月 22

バージョン	説明	セクション	ステータス	日付
	。			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。

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。