Cisco IOS および IOS XE ソフトウェアの Cluster Management Protocol のサービス妨害（DoS）の脆弱性

High

アドバイザリーID : cisco-sa-20190327-cmp-dos
初公開日 : 2019-03-27 16:00
バージョン 1.0 : Final
CVSSスコア : 7.4
回避策 : No workarounds available
Cisco バグ ID : CSCvj25124 CSCvj25068

CVE-2019-1746

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 IOS ソフトウェアおよび Cisco IOS XE ソフトウェアのクラスタ管理プロトコル（CMP）処理コードに含まれる脆弱性により、認証されていない隣接する攻撃者がサービス妨害（DoS）状態を引き起こす可能性があります。

この脆弱性は、CMP 管理パケットの処理時に入力が十分に検証されないことに起因しています。攻撃者は、悪意のある CMP 管理パケットを該当デバイスに送信することによって、本脆弱性をエクスプロイトできる可能性があります。エクスプロイトに成功すると、スイッチがクラッシュしてサービス妨害（DoS）状態に陥る危険性があります。スイッチは自動的にリロードされます。

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-20190327-cmp-dos

このアドバイザリは、2019 年 3 月 27 日に公開された Cisco IOS ソフトウェアおよび IOS XE ソフトウェア リリースのセキュリティ アドバイザリ バンドルの一部です。このバンドルには、19 件の脆弱性に関して 17 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: March 2019 Semiannual Cisco IOS and IOS XE 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

スイッチが次のすべての条件を満たす場合、この脆弱性は、該当リリースの Cisco IOS または IOS XE ソフトウェアを実行している Cisco Catalyst スイッチに影響を及ぼします。

- CMP が有効になっている。一部のプラットフォームでは、CMP がデフォルトで有効になっています。
- スイッチがクラスタ ドメインの一部に設定されている。
- スイッチが、コマンド スイッチまたはメンバー スイッチのロールを持つ。

脆弱性が存在する Cisco IOS ソフトウェアおよび IOS XE 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。

スイッチに脆弱性を持つ設定があるかどうかの確認

スイッチに脆弱性を持つ設定があるかどうかは、2 つの方法で確認できます。

オプション1:show cluster | include cluster コマンドの使用

デバイスの CMP ステータスを特定し、クラスタ メインの一部に設定されていることを確認するには、show cluster | include cluster 特権 EXEC コマンドをデバイスで使用します。次の例は、show cluster | include cluster コマンドを CMP が有効でクラスタ ドメインの一部にも設定されている Cisco Catalyst スイッチで実行した場合の出力です。

<#root>

SWITCH#

show cluster | include cluster

<ROLE> for cluster <CLUSTER_NAME>

このコマンドが存在しない場合、またはその他の出力が生成される場合、デバイスはこのアドバイザリで説明されている脆弱性の影響を受けていません。

オプション2:show running-config [all]コマンドの使用

CMP が有効になっている状態でデバイスが設定されているかどうかを確認するには、show running-config all | include cluster run 特権 EXEC コマンドをデバイスで使用します。以下は、show running-config all の出力例です。 | include cluster run コマンドを CMP が有効になっているスイッチで使用します。

```
<#root>

SWITCH#

show running-config all | include cluster run
  cluster run
```

デバイスがコマンド スイッチまたはメンバー スイッチとしてクラスタ ドメインの一部に設定されているかどうかを判別するには、show running-config | include cluster commander|cluster member特権EXECコマンドを使用します。クラスタ ドメインの一部ではないスイッチでは、このコマンドの出力が空になります。

以下に、show running-config | include cluster commander|cluster memberコマンドを、コマンドスイッチのロールを持つクラスタドメインの一部として設定されているデバイスで実行した場合の出力例を示します。

```
<#root>

SWITCH#

show running-config | include cluster commander|cluster member

cluster member <NUMBER>

 mac-address

 <MAC-ADDRESS>
```

以下に、show running-config | include cluster commander|cluster memberコマンドの出力例を示します。

```
<#root>

SWITCH#

show running-config | include cluster commander|cluster member

cluster commander-address

 <MAC-ADDRESS> <CLUSTER-INFORMATION>
```

オプション 2 を使用してデバイスを評価する場合、次の両方の条件に該当する場合にのみ、デバイスはこのアドバイザリで説明されている脆弱性の影響を受けています。

- show running-config all | include cluster run コマンドの出力には、次の正確な文字列が含まれます。

cluster run
- NAT が設定にあるかどうかを判断するには、脆弱性がある次の設定例に示すように show running-config | include cluster commander|cluster memberコマンドの出力が空になることはありません。

Cisco IOS ソフトウェア リリースの判別

デバイス上で実行されている Cisco IOS ソフトウェア リリースは、管理者がデバイスにログインして、CLI で show version コマンドを使用し、表示されるシステム バナーを参照することにより確認できます。デバイスが Cisco IOS ソフトウェアを実行している場合、システム バナーに「Cisco Internetwork Operating System Software」や「Cisco IOS Software」などのテキストが表示されます。バナーにはインストールされたイメージ名もカッコ内に表示され、その後ろに、Cisco IOS ソフトウェアのリリース番号とリリース名が表示されます。一部のシスコデバイスでは、show version コマンドをサポートしていなかったり、別の出力が表示されたりします。

次に、Cisco IOS ソフトウェア リリース 15.5(2)T1 が実行されていて、インストールされているイメージ名が C2951-UNIVERSALK9-M であるデバイスでのコマンド出力例を示します。

<#root>

```
Router>
show version

Cisco IOS Software, C2951 Software (C2951-UNIVERSALK9-M), Version 15.5(2)T1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Mon 22-Jun-15 09:32 by prod_rel_team
.
.
.
```

Cisco IOS ソフトウェア リリースの命名と番号付けの規則に関する詳細は、『Cisco IOS and NX-OS Software Reference Guide』を参照してください。

Cisco IOS XE ソフトウェア リリースの判別

デバイス上で実行されている Cisco IOS XE ソフトウェア リリースは、管理者がデバイスにログインして、CLI で show version コマンドを実行し、表示されるシステム バナーを参照することにより確認できます。デバイスが Cisco IOS XE ソフトウェアを実行している場合、システム バナーに「Cisco IOS Software」、「Cisco IOS XE Software」などのテキストが表示されます。

次に、Cisco IOS XR ソフトウェア リリース 16.2.1 が実行されていて、インストールされてい

るイメージ名が CAT3K_CAA-UNIVERSALK9-M であるデバイスでのコマンドの出力例を示します。

```
<#root>

ios-xe-device#

show version


Cisco IOS Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version Denali 16.2.1, REL
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Sun 27-Mar-16 21:47 by mcpre
.
.
.
```

Cisco IOS XE ソフトウェア リリースの命名と番号付けの規則に関する詳細は、『Cisco IOS and NX-OS Software Reference Guide』を参照してください。

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 Cisco IOS XR ソフトウェアまたは Cisco NX-OS ソフトウェアには影響を与えないことを確認しました。

詳細

CMP は、単一の IP アドレスによるスイッチ グループの管理を容易にする基盤技術の集合体です。

各クラスタには、「コマンド スイッチ」と呼ばれるマスター スイッチが存在し、残りのスイッチはメンバー スイッチとして機能します。コマンド スイッチは、クラスタ全体に対する主要な管理インターフェイスを提供します。クラスタ ドメイン内のスイッチは CMP を使用してすべてのシグナリング操作および設定操作を実行します。CMP は、シスコの組織固有識別子（OUI）と CMP プロトコル識別子を持つサブネットワーク アクセス プロトコル（SNAP）ヘッダーを含むカプセル化イーサネット フレームを使用します。

この脆弱性は、CMP 管理パケットの処理時に入力が十分に検証されないことに起因しています。CMP のレイヤ 2 の性質上、標的とされるデバイスが存在するローカル ネットワーク セグメントへのアクセス権を持つ攻撃者だけが、このアドバイザリで説明されている脆弱性をエクスプロイトできます。エクスプロイトに成功すると、スイッチがクラッシュしてサービス妨害（DoS）状態に陥る危険性があります。スイッチは自動的にリロードされます。

セキュリティ侵害の痕跡

この脆弱性がエクスプロイトされると、該当スイッチで、次のような エラー メッセージが生成される可能性があります。

```
Mar 22 2019 10:18:29.180 EST: %DATACORRUPTION-CLUSTER_MEMBER_2-1-DATAINCONSISTENCY: copy error,  -PC= 0
-Traceback= 463F74z 486D64z 2B8F2D8z 2A9E20z 2A7C74z 2A7EE8z 297DD08z 297A088z
Mar 22 2019 10:18:33.385 EST: %SYS-CLUSTER_MEMBER_2-3-TIMERNEG: Cannot start timer (0x48D3988) with nega
-Traceback= 463F74z 1F2230 4z 2A17DCz 297DD08z 297A088z
Unexpected exception to CPU vector 1 (undefined instruction), PC = 2
-Traceback= 0x2z 0x31EC60z 0x1655CF4z
```

-Traceback= テキストの後に表示される値はバージョンによって異なります。脆弱性のエクスプロイトによってデバイスが侵害を受けているかどうかは、サポート担当部門に連絡し、エラーメッセージを調査することで判断できます。

回避策

この脆弱性に対処する回避策はありません。

CMP を無効にすると攻撃ベクトルを排除できます。CMP を無効化するには、no cluster run コマンドをグローバル コンフィギュレーション モードで使用します。脆弱性を修正したアップグレードが提供されるまでは、この処置が最善策になります。

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、[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、本アドバイザリの URL をご用意ください。

Cisco IOS および IOS XE ソフトウェア

お客様が Cisco IOS ソフトウェアおよび IOS XE ソフトウェアの脆弱性による侵害の可能性を判断するため、シスコは Cisco IOS Software Checker ツールを提供しています。このツールを使用すると、特定のソフトウェア 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リ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リ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。

このツールを使用して次のタスクを実行できます。

- ドロップダウン リストからリリース（複数可）を選択するか、分析対象となるローカル システムからファイルをアップロードして、検索を開始する
- show version コマンドの出力をツールで解析する
- カスタマイズした検索（過去に公開されたすべてのシスコ セキュリティ アドバイザリを検索対象に入れたり、特定のアドバイザリのみ、または最新のバンドル資料のすべてのアドバイザリを含めるなど）を作成する

リリースが、公開されたシスコ セキュリティ アドバイザリのいずれかに該当するかどうかを確認するには、Cisco.com の Cisco IOS Software Checker を使用するか、以下のフィールドに Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェアリリース（たとえば、15.1(4)M2、3.13.8S など）を入力します。

	オン

デフォルトでは、Cisco IOS ソフトウェアのチェックには、結果は、高セキュリティへの影響の評価 (サー) または重大な脆弱性にのみが含まれています。「中間」の SIR 脆弱性の結果を含めるには、Cisco.com の Cisco IOS ソフトウェア チェッカーを使用して、[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 IOS XE ソフトウェア リリースと Cisco IOS ソフトウェア リリースのマッピングについては、Cisco IOS XE ソフトウェアのリリースに応じて「Cisco IOS XE 2 Release Notes」、「Cisco IOS XE 3S Release Notes」、または「Cisco IOS XE 3SG Release Notes」を参照してください。

注：Cisco IOS XE ソフトウェアリリース 16.9.1 以降では、アップグレードにスマートライセンスが必要です。Cisco IOS XE をリリース 16.9.1 以降にアップグレードする予定がある場合は、スマート ライセンス要件を検討することをお勧めします。スマートライセンスの詳細については、 こちらの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) 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

この脆弱性は Cisco TAC サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190327-cmp-dos

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	2019 年 3 月 27 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。