Cisco IOS XE ソフトウェア Web UI のサービス妨害（DoS）の脆弱性

アドバイザリーID : cisco-sa-20180926-webuidos
初公開日 : 2018-09-26 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 : CSCva31961

CVE-2018-0469

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 XE ソフトウェアの Web ユーザ インターフェイスの脆弱性により、認証されていないリモート攻撃者が影響を受けるデバイスのリロードを引き起こす可能性があります。この脆弱性は、特定の HTTP 要求を処理するときの影響を受けるソフトウェアによるメモリの二重解放処理が原因で発生します。

攻撃者は、影響を受けるソフトウェアの Web ユーザ インターフェイスに特定の HTTP 要求を送信することで、この脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功すると、攻撃者が影響を受けるデバイスのリロードを引き起こし、影響を受けるデバイスでサービス妨害（DoS）状態が発生する可能性があります。この脆弱性をエクスプロイトするには、攻撃者は影響を受けるソフトウェアの管理インターフェイス（通常は制限付き管理ネットワークに接続されている）にアクセスできる必要があります。

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-20180926-webuidos

このアドバイザリは、2018 年 9 月 26 日に公開された 13 件の脆弱性に関する 12 件のシスコ セキュリティ アドバイザリを含む 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 アドバイザリ公開資料の一部です。アドバイザリとリンクの一覧については、『Cisco Event Response: September 2018 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

HTTP サーバ機能が有効になっている場合、この脆弱性は、Cisco IOS XE ソフトウェアの脆弱性が存在するリリースを実行している Cisco Catalyst 3650 および 3850 シリーズ スイッチに影響を及ぼします。HTTP サーバ機能のデフォルトの状態は、バージョンによって異なります。

本脆弱性は、Cisco IOS XE リリース 16.1.1 で取り込まれました。脆弱性が存在する Cisco IOS XE 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」セクションを参照してください。

HTTP サーバ設定の確認

HTTP サーバ機能がデバイスで有効かどうかを確認するには、管理者がデバイスにログインして CLI で show running-config | include http (secure|server)コマンドを使用して、グローバルコンフィギュレーションにip http serverコマンドまたはip http secure-serverコマンドが含まれるかどうかを確認します。どちらかのコマンドが含まれ、設定されている場合は、HTTP サーバ機能が有効です。

以下に、show running-config | include http (secure|server)コマンドの出力を示します。

<#root>

```
Router#
show running-config | include http (secure|server)


ip http server
ip http secure-server
```

前述のコマンドの出力に次の内容も含まれている場合

<#root>

```
ip http active-session-modules none
ip http secure-active-session-modules none
```

そのデバイスはエクスプロイト可能ではありません。

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 ソフトウェア、Cisco IOS XR ソフトウェア、および 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

この脆弱性には、認証ベクトルが「Not Required」の CVSSv3 スコアが付いています。 16.2.2 より前の Cisco IOS XE のリリースでは、この脆弱性をエクスプロイトするための認証は不要でした。Cisco IOS XE ソフトウェア リリース 16.2.2 以降は、この脆弱性をエクスプロイトするための認証が必要です。

セキュリティ侵害の痕跡

Cisco IOS XE ソフトウェア リリース 16.2.2 syslog には、Web GUI の「Login Successful」メッセージが表示されていて、その後に次の syslog メッセージが続いている必要があります。

```
%PMAN-3-PROCHOLDDOWN: The process dbm has been helddown (rc 134)
```

16.2.2 より前の Cisco IOS XE ソフトウェア リリースでは「Login Successful」メッセージは表示されず、前述のメッセージの syslog メッセージだけが表示されます。

回避策

この脆弱性に対処する回避策はありません。

Web GUI を有効にする必要がないお客様は、次のようにして無効化できます。

<#root>

```
Switch#configure terminal
Switch(config)#
```

no ip http server

```
Switch(config)#
```

no ip http secure-server

```
Switch(config)#exit
Switch#
```

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。

Check

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。

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-20180926-webuidos

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	2018 年 9 月 26 日

利用規約

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。