Cisco IOSソフトウェアのTFTPサーバにおけるDoS脆弱性

アドバイザリーID : cisco-sa-20150722-tftp CVE-2015-0681
初公開日 : 2015-07-22 16:00
バージョン 1.0 : Final
CVSSスコア : 7.1
回避策 : No Workarounds available
Cisco バグ ID : CSCts66733

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およびCisco IOS XEソフトウェアのTFTPサーバ機能の脆弱性により、認証されていないリモートの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。

TFTPサーバ機能は、デフォルトでは有効になっていません。

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。

この脆弱性に対しては回避策があります。

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-20150722-tftp

該当製品

脆弱性のある製品

該当するバージョンのソフトウェアを実行しているCisco IOSおよびCisco IOS XEソフトウェアデバイスは、デバイスにTFTPサーバが設定されている場合に脆弱性が存在します。

デバイスにTFTPサーバが設定されているかどうかを確認するには、 show running-config | include ^tftp-serverコマンドラインインターフェイスexecコマンドを使用します。デバイスにTFTPサーバが設定されていない場合、このコマンドは出力を返しません。 デバイスにTFTPサ

ーバが設定されている場合、出力にはキーワード tftp-serverで始まる1行または複数行が表示されます。 次の例では、TFTPサーバが有効になっていません。

```
Router#show running-config | include ^tftp-server
Router#
```

次の例では、TFTPサーバが有効になっています。

```
Router#show running-config | include ^tftp-server
tftp-server flash:c2800nm-adventerprisek9-mz.124-1
tftp-server flash:
Router#
```

シスコ製品で稼働している Cisco IOS ソフトウェア リリースを確認するには、デバイスにログインして show version コマンドを使って、システム バナーを表示します。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た場合は、デバイスが Cisco IOS ソフトウェアを実行しています。カッコ内にイメージ名が表示され、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続きます。他のシスコ デバイスでは、show version コマンドが存在しなかったり、別の出力が表示されたりします。

次の例は、Cisco IOS ソフトウェア リリースが 15.2(4)M5、インストールされたイメージ名が C3900-UNIVERSALK9-M であるシスコ製品を示しています。

<#root>

```
Router>
```

show version

```
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.2(4)M5, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Fri 13-Sep-13 16:44 by prod_rel_team
```

!--- output truncated

Cisco IOSソフトウェアのリリース命名規則の追加情報は、『White Paper: Cisco IOS and NX-OS Software Reference Guide』で確認できます。

脆弱性を含んでいないことが確認された製品

次の製品はこの脆弱性の影響を受けないことが確認されています。

- Cisco IOS XR ソフトウェア
- Cisco NX-OS ソフトウェア

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

詳細

Cisco IOSおよびCisco IOS XEソフトウェアのTFTPサーバ機能の脆弱性により、認証されていないリモートの攻撃者がデバイスのリロードまたはハングを引き起こす可能性があります。

この脆弱性は、TFTP要求を処理する際のメモリ管理が不適切であることに起因します。攻撃者は、該当デバイスに対して多数のTFTP要求を行うことで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者はデバイスのリロードまたはハングを引き起こす可能性があります。

Cisco IOSソフトウェアおよびCisco IOS XEソフトウェアを実行し、TFTPサーバが有効になっているデバイスが影響を受けます。

この脆弱性は、Cisco Bug ID CSCts66733(登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposure(CVE)IDとしてCVE-2015-0681が割り当てられています。

この脆弱性に対するエクスプロイトコードは存在しますが、プラットフォームとソフトウェアバージョン間でコードが一貫して実行されるわけではありません。

回避策

TFTPアクセスリスト

警告：この脆弱性の機能はトランスポートとしてUDPを使用するため、送信元のIPアドレスをスプーフィングする可能性があり、信頼できるIPアドレスからこれらのポートへの通信を許可するアクセスコントロールリスト(ACL)を無効にする可能性があります。より有効な緩和策として、ユニキャストRPFとTFTPアクセスリストの併用を検討してください。

次のTFTP ACLの例は、ベストプラクティスとして、導入されたCisco IOS TFTPサーバの一部として含める必要があります。

```
!---

!--- Define requesting segments or individual hosts

!--- The following example allows hosts on network 192.168.22.X to

!--- make TFTP requests to the router.

!---

access-list 1 permit 192.168.22.0 0.0.0.255
```

TFTPサーバを使用してサービスを提供する各ファイルを、 tftp-server文の最後にACL番号を含めることによって、TFTP ACLにアンカーします。

```
tftp-server flash:c2800nm-adventerprisek9-mz.124-1 1
```

TFTPサーバを完全に無効にする

Cisco IOSソフトウェアは、別のTFTPサーバが使用できない場合にCisco IOSイメージを転送するのに役立つTFTPサーバ機能を提供します。TFTPサーバの機能が現在必要でない場合は、次の手順を実行してTFTPサーバを無効にすることができます。

1. ルータがイネーブルモードの場合、show running-configコマンドを発行して、tftp-serverで始まる行を探します。
2. tftp-serverで始まる各行をコピーして、テキストエディタに貼り付けます。
3. 各行の先頭に単語noを付け、その後にスペースを1つ付加します。
4. 編集した各行をコピーし、コンフィギュレーションモードのルータで、コピーした行をコンフィギュレーションに貼り付けます。
5. コンフィギュレーションモードを終了し、コマンドshow running-configを発行して、tftp-serverで始まる行を探します。
6. 出力に行がないことを確認します。
7. 新しい設定を保存します。

修正済みソフトウェア

Cisco IOS ソフトウェア

シスコは、お客様がCisco IOSソフトウェアの脆弱性の影響を受けるかどうかを判断するためのツールを提供しています。 Cisco IOS Software Checker により、次のタスクを実行できます。

- ドロップダウン メニューからリリースを選択するか、ローカル システムからファイルをアップロードすることによって、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を作成し、以前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含めるか、特定の資料を含める

このツールは、クエリされたソフトウェアリリースに影響を与えるシスコセキュリティアドバイザリと、各シスコセキュリティアドバイザリのすべての脆弱性を修正する最初のリリース(First Fixed)を特定します。適用可能な場合、表示されているすべてのアドバイザリのすべての脆弱性を修正する最初のリリース(Combined First Fixed)も返します。Cisco IOS Software Checkerを参照してください。

Cisco IOS XE ソフトウェア

Cisco IOS XEソフトウェアは、このアドバイザリに記載されている脆弱性の影響を受けます。

Cisco IOS ソフトウェア リリースへの Cisco IOS XE ソフトウェア リリースのマッピングについては、「 Cisco IOS XE 2 Release Notes」、「 Cisco IOS XE 3S Release Notes」、および「 Cisco IOS XE 3SG Release Notes」を参照してください。

Cisco IOS XE ソフトウェア リリース	First Fixed Release（修正された最初のリリース）
2.5.x	脆弱性あり、3.6.0S以降に移行
2.6.x	脆弱、3.6.0S以降に移行
3.1.xS	脆弱、3.6.0S以降に移行
3.1.xSG	脆弱性あり、3.4.0SG以降に移行
3.2.xS	脆弱、3.6.0S以降に移行
3.2.xSE	脆弱性あり、3.3.0SE以降に移行
3.2.xSG	脆弱性あり、3.4.0SG以降に移行
3.2.xXO	脆弱性あり、3.3.0XO以降に移行
3.2.xSQ	脆弱性あり、サポート組織に連絡
3.3.xS	脆弱、3.6.0S以降に移行
3.3.xSE	脆弱性なし
3.3.xSG	脆弱性あり、3.4.0SG以降に移行

3.3.xXO	脆弱性なし
3.3.xSQ	脆弱性あり、サポート組織に連絡
3.4.xS	脆弱、3.6.0S以降に移行
3.4.xSG	脆弱性なし
3.4.xSQ	脆弱性あり、サポート組織に連絡
3.5.xS	脆弱、3.6.0S以降に移行
3.5.xE	脆弱性なし
3.6.xS	脆弱性なし
3.6.xE	脆弱性なし
3.7.xS	脆弱性なし
3.7.xE	脆弱性なし
3.8.xS	脆弱性なし
3.9.xS	脆弱性なし
3.10.xS	脆弱性なし
3.11.xS	脆弱性なし
3.12.xS	脆弱性なし
3.13.xS	脆弱性なし
3.14.xS	脆弱性なし
3.15.xS	脆弱性なし

推奨事項

$propertyAndFields.get("recommendations")

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。

この脆弱性はシスコ内部でのテストによって発見され、チームvhunterのZhangzhibingもこの脆弱性を発見して、公開されているエクスプロイトコードを開発しました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150722-tftp

改訂履歴

リビジョン 1.0	2015年7月22日	初回公開リリース

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。