Cisco IOSソフトウェアおよび IOS XE ソフトウェア TCPパケット メモリリーク の 脆弱性

High

アドバイザリーID : cisco-sa-20150325-tcpleak

CVE-2015-0646

初公開日 : 2015-03-25 16:00

最終更新日 : 2016-01-14 17:24

バージョン 1.2 : Final

CVSSスコア : 7.8

回避策 : No workarounds available

Cisco バグ ID : CSCum94811

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 TCP 入力 モジュールの脆弱性は非認証、リモート攻撃者により影響を受けたデバイスのメモリリークおよび終局リロードを引き起こすことを可能にする可能性があります。

脆弱性は TCP 3 ウェイ ハンドシェイクの確立で使用されるある特定の巧妙に細工された パケット シーケンスの不適当な処理が原因です。 攻撃者は TCP パケットの巧妙に細工された シーケンスの送信によって 3方向ハンドシェイクを確立している間この脆弱性を不正利用する可能性があります。 正常な エクスプロイトは攻撃者により影響を受けたデバイスのメモリリークおよび終局リロードを引き起こすことを可能にする可能性があります。

この脆弱性に対する回避策はありません。

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。このアドバイザリは、次のリンクより確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-tcpleak

注: 2015 年 3 月 25 日、Cisco IOS ソフトウェアおよび IOS XE ソフトウェアのセキュリティ アドバイザリにおいて、7 つの Cisco Security Advisory を含むバンドル資料を公開しました。 これらのアドバイザリは Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアの脆弱性を扱っています。 個々の公表資料へのリンクは、次のリンクにある「*シスコのイベント対応： Cisco IOS および IOS XE ソフトウェアに関するセキュリティ アドバイザリ公開資料*」に掲載されています。

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar15.html

該当製品

脆弱性のある製品

影響を受けた Cisco IOSソフトウェアか Cisco IOS XE ソフトウェアを実行している Ciscoデバイスは脆弱です。 Cisco IOS を実行するあらゆる TCPポートで受信するあらゆるプロセスで設定される Ciscoデバイスか Cisco IOS XE ソフトウェアは可能性としては影響を受けています。 TCP ポートで受信するために設定することができる Cisco IOSソフトウェアに多重プロセスがあります。 そのような設定されたプロセスの例は HTTP、HTTPS、SSH、または Telnet です。 他の設定されたプロセスは影響を受けたデバイスにあり、TCP ポートで受信するかもしれません。 TCP 受信プロセスのうちのどれかが Ciscoデバイスで有効に なるかどうか判別するのに必要な設定は設定されたプロセスに特定です。

ある特定の実行するデバイス Cisco IOS および Cisco IOS XE ソフトウェアでどのプロセスでも TCP ポートで受信したかどうか確認することは可能性のあるです。 Cisco IOSデバイスまたは Cisco IOS XE デバイスが受信サービスに向かう TCP パケットを処理するかどうか判別するためにデバイスにログイン し、次の Command Line Interface （ CLI ）コマンド **show tcp 要約すべて**の発行するか、または **コントロール・プレーン ホスト 開港を示して下さい**。 出力があらゆる TCP ポートで受信するプロセスを表示したもので場合デバイスは脆弱です。

次の例はこの脆弱性から影響を受ける Cisco IOSデバイスを示したものです。 デバイスは TCP ポート 80 および 22 で受信するプロセスがあるので脆弱です:

```
Router#show control-plane host open-ports
Active internet connections (servers and established)
Prot                Local Address             Foreign Address                   Service    State
 tcp                        *:22                      *:0                  SSH-Server   LISTEN
 tcp                        *:22                      *:0                  SSH-Server   LISTEN
 tcp                        *:80                      *:0                   HTTP CORE   LISTEN
 tcp                        *:80                      *:0                   HTTP CORE   LISTEN
 udp                       *:161                      *:0                     IP SNMP   LISTEN
 udp                       *:162                      *:0                     IP SNMP   LISTEN
 udp                     *:53519                      *:0                     IP SNMP   LISTEN
Router#

Router#show tcp brief all
TCB       Local Address           Foreign Address        (state)
03577CD8  ::.22                    *.*                    LISTEN
03577318  *.22                    *.*                    LISTEN
035455F8  ::.80                    *.*                    LISTEN
03544C38  *.80                    *.*                    LISTEN
Router#
```

注: CLI コマンド **show tcp 要約はすべてコントロール・プレーン ホスト 開港が**依存したプラットフォームで、Cisco IOS か Cisco IOS XE ソフトウェアを実行するすべてのプラットフォームに現在ではないかもしれないことを 示し。

シスコ製品上で動作している Cisco IOS ソフトウェア リリースについては、管理者がデバイスにログインして **show version** コマンドを発行し、システム バナーを表示することで判別できます。 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。

```
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
```

```
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
```

Cisco IOS ソフトウェア リリースの命名規則については、以下を参照してください。[ホワイトペーパー： Cisco IOS および NX-OS ソフトウェア リファレンス ガイド]

脆弱性を含んでいないことが確認された製品

Cisco IOS XR ソフトウェアはこの脆弱性から影響を受けません。

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 TCP 入力 モジュールの脆弱性は非認証、リモート攻撃者により影響を受けたデバイスのメモリリークおよび終局リロードを引き起こすことを可能にする可能性があります。

脆弱性は TCP 3 ウェイ ハンドシェイクの確立で使用されるある特定の巧妙に細工された パケット シーケンスの不適当な処理が原因です。 攻撃者は TCP パケットの巧妙に細工された シーケンスの送信によって 3方向ハンドシェイクを確立している間この脆弱性を不正利用する可能性があります。 正常なエクスプロイトは攻撃者により影響を受けたデバイスのメモリリークおよび終局

リロードを引き起こすことを可能にする可能性があります。

この脆弱性は IPv4 および IPv6 両方パケットを使用して不正利用することができます。 脆弱性は3方向ハンドシェイクの確立の間に TCP パケットの巧妙に細工された シーケンスによって引き起こすことができます。 TCP パケットの巧妙に細工された シーケンスはデバイスで設定されるあらゆるインターフェイスの IPv4 または IPv6 ユニキャスト アドレスを使用してあらゆる TCP リスニングポートに向かう必要があります。

この脆弱性は影響を受けたデバイスに向かうトラフィックによってしか引き起こし、影響を受けたデバイスを通過するトラフィックと不正利用することができません。

脆弱 な 設定の基準を満たすデバイスでは、TCP パケットの巧妙に細工された シーケンスはこの脆弱性を引き起こす可能性があります。 インフラストラクチャのナレッジの攻撃者はこの脆弱性を不正利用するためにある特定の条件の TCP パケットを細工 する可能性があります。

この脆弱性 Cisco バグ ID CSCum94811 （ 登録ユーザのみ ）で文書化されています、よくある脆弱性および公開（CVE）ID CVE-2015-0646 は割り当てられました。

セキュリティ侵害の痕跡

回避策

この脆弱性に対する回避策はありません。

ネットワーク内のシスコ デバイスに適用可能な他の対応策は、このアドバイザリの付属ドキュメントである『Cisco Applied Mitigation Bulletin』を参照してください。以下のリンクから入手できます。
http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=37433

修正済みソフトウェア

ソフトウェアのアップグレードを検討する場合は、 http://www.cisco.com/go/psirt の Cisco Security Advisories, Responses, and Alerts アーカイブや、後続のアドバイザリを参照して侵害の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。

Cisco IOS ソフトウェア

シスコでは、Cisco IOS ソフトウェアの脆弱性にさらされてい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（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、特定の資料のみ、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

このツールを使うことで、そのソフトウェア リリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース（"First Fixed"）を特定できます。 また該当する場合、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。 Cisco IOS Software Checker を参照するか、次のフィールドに Cisco IOS ソフトウェア リリースを入力して、いずれかの公開された Cisco IOS ソフトウェア アドバイザリに該当するかどうかを判断できます。

（入力例： 15.1(4)M2）

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

Cisco IOS XE ソフトウェアはこのアドバイザリに記載される脆弱性から影響を受けます。

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）	2015 年 3 月 の Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドル パブリケーションのすべてのアドバイザリに対する First Fixed Release（修正された最初のリリース）
2.5.x	脆弱性なし	脆弱性あり; 3.12.3S 以降へ移行
2.6.x	脆弱性なし	脆弱性あり; 3.12.3S 以降へ移行
3.1.xS	脆弱性なし	脆弱性あり; 3.12.3S 以降へ移行
3.1.xSG	脆弱性なし	脆弱性なし
3.2.xS	脆弱性なし	脆弱性あり; 3.12.3S 以降

		へ移行
3.2.xSE	脆弱性なし	脆弱性あり; migrate to 3.7.1E or later.
3.2.xSG	脆弱性なし	脆弱性なし
3.2.xXO	脆弱性なし	脆弱性なし
3.2.xSQ	脆弱性なし	脆弱性なし
3.3.xS	脆弱性なし	脆弱性あり; 3.12.3S 以降へ移行
3.3.xSE	脆弱性なし	脆弱性あり; migrate to 3.7.1E or later.
3.3.xSG	脆弱性なし	脆弱性あり; migrate to 3.7.1E or later.
3.3.xXO	脆弱性あり; 3.7.0E またはそれ以降への移行する。	脆弱性あり; migrate to 3.7.1E or later.
3.3.xSQ	脆弱性なし	脆弱性なし
3.4.xS	脆弱性なし	脆弱性あり; 3.12.3S 以降へ移行
3.4.xSG	脆弱性なし	脆弱性あり; migrate to 3.7.1E or later.
3.4.xSQ	脆弱性なし	脆弱性なし
3.5.xS	脆弱性なし	脆弱性あり; 3.12.3S 以降へ移行
3.5.xE	脆弱性あり; 3.7.0E またはそれ以降への移行する。	脆弱性あり; migrate to 3.7.1E or later.
3.6.xS	脆弱性なし	脆弱性あり; 3.12.3S 以降へ移行
3.6.xE	脆弱性あり; 3.7.0E またはそれ以降への移行する。	脆弱性あり; migrate to 3.7.1E or later.
3.7.xS	脆弱性なし	脆弱性あり; 3.12.3S 以降へ移行
3.7.xE	脆弱性なし	3.7.1E
3.8.xS	脆弱性あり; 3.10.5S またはそれ以降への移行する。	脆弱性あり; 3.12.3S 以降へ移行
3.9.xS	脆弱性あり; 3.10.5S またはそれ以降への移行する。	脆弱性あり; 3.12.3S 以降へ移行
3.10.xS	3.10.5S	脆弱性あり; 3.12.3S 以降へ移行

3.11.xS	脆弱性あり; 3.12.3S 以降へ移行	脆弱性あり; 3.12.3S 以降へ移行
3.12.xS	3.12.3S	脆弱性あり; 3.12.3S 以降へ移行
3.13.xS	脆弱性なし	3.13.2S
3.14.xS	脆弱性なし	脆弱性なし
3.15.xS	脆弱性なし	脆弱性なし

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。

この脆弱性はサポート ケースの解決の間に検出されました。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-tcpleak

改訂履歴

Version	Description	Section	Status	日付
1.2	過去に公開されたすべてのCisco IOSソフトウェア セキュリティ アドバイザリを照会できる Cisco IOS Checker ソフトウェアの Checker フォームを更新しました。			2016 年 1 月 14 日
1.1	2015 年 3 月 の Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドル パブリケーションのすべてのアドバイザリにおいて First Fixed Release（修正した最初のリリース）の箇所を更新しました。			2015 年 3 月 25 日
1.0	初回公開リリース			2015 年 3 月 25 日

利用規約

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。