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

アドバイザリーID : cisco-sa-20150325-tcpleak
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

CVE-2015-0646

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により、認証されていないリモート攻撃者が該当デバイスのメモリリークを引き起こし、最終的にリロードを引き起こす可能性があります。

この脆弱性は、TCP 3ウェイハンドシェイクの確立に使用される特定の巧妙に細工されたパケットシーケンスの不適切な処理に起因します。攻撃者は、3ウェイハンドシェイクの確立中に、巧妙に細工されたTCPパケットシーケンスを送信することで、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者は該当デバイスのメモリリークを引き起こし、最終的にリロードを引き起こす可能性があります。

この脆弱性に対する回避策はありません。

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-20150325-tcpleak

注： 2015年3月25日のCisco IOSおよびXEソフトウェアセキュリティアドバイザリバンドル公開には7件のCisco Security Advisoryが含まれています。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。個々の公開リンクは、次のリンクにある『Cisco Event Response: Semiannual Cisco IOS & XE Software Security Advisory Bundled Publication』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

該当するCisco IOSソフトウェアまたはCisco IOS XEソフトウェアを実行しているシスコデバイスには脆弱性が存在します。Cisco IOSまたはCisco IOS XEソフトウェアを実行し、TCPポートをリスニングするプロセスが設定されているシスコデバイスは、この脆弱性の影響を受ける可能性があります。Cisco IOSソフトウェアには、TCPポートをリッスンするように設定できる複数のプロセスがあります。このような設定済みプロセスの例としては、HTTP、HTTPS、SSH、Telnetなどがあります。影響を受けるデバイス上に他の設定済みプロセスが存在し、TCPポートをリッスンしている可能性があります。シスコデバイスでTCPリスニングプロセスのいずれかが有効になっているかどうかを確認するために必要な設定は、設定されたプロセスに固有です。

Cisco IOSおよびCisco IOS XEソフトウェアを実行する特定のデバイスでは、TCPポートでリスニングしているプロセスがあるかどうかを判別できます。Cisco IOSデバイスまたはCisco IOS XEデバイスがリスニングサービス宛てのTCPパケットを処理するかどうかを判別するには、デバイスにログインして、次のコマンドラインインターフェイス(CLI)コマンド show tcp brief allまたは show control-plane host open-portsのいずれかを発行します。出力にTCPポートをリスニングしているプロセスが示されている場合、そのデバイスには脆弱性が存在します。

次の例は、この脆弱性の影響を受けるCisco IOSデバイスを示しています。デバイスは、TCPポート80および22でリッスンしているプロセスがあるため、脆弱です。

<#root>

```
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 brief all および show control-plane host open-ports はプラットフォームに依存し、Cisco IOSまたはCisco IOS XEソフトウェアを実行しているすべてのプラットフォームに存在するとは限りません。

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

Cisco IOS XRソフトウェアは、この脆弱性の影響を受けません。

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により、認証されていないリモート攻撃者が該当デバイスのメモリリークを引き起こし、最終的にリロードを引き起こす可能性があります。

この脆弱性は、TCP 3ウェイハンドシェイクの確立に使用される特定の巧妙に細工されたパケットシーケンスの不適切な処理に起因します。攻撃者は、3ウェイハンドシェイクの確立中に、巧妙に細工されたTCPパケットシーケンスを送信することで、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者は該当デバイスのメモリリークを引き起こし、最終的にリロードを引き起こす可能性があります。

この脆弱性は、IPv4 パケットまたは IPv6 パケットのどちらでも不正利用される可能性があります。この脆弱性は、3ウェイハンドシェイクの確立中に巧妙に細工されたTCPパケットシーケンスによってトリガーされる可能性があります。巧妙に細工されたTCPパケットのシーケンスは、デバイスに設定された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、TCPリスニングポート宛てに送信される必要があります。

この脆弱性は、該当デバイス宛てのトラフィックによってのみトリガーされ、該当デバイスを通過するトラフィックによっては不正利用されません。

脆弱性のある設定基準を満たすデバイスでは、巧妙に細工された一連のTCPパケットによってこの脆弱性が引き起こされる可能性があります。インフラストラクチャの知識を持つ攻撃者は、特定の条件を持つTCPパケットを作成して、この脆弱性を不正利用する可能性があります。この脆弱性の不正利用に成功した場合、影響を受けた機器では再起動が発生することがあります。

この脆弱性は、Cisco Bug ID CSCum94811(登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2015-0646が割り当てられています。

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。
https://sec.cloudapps.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、お客様が 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。

(例：15.1(4)M2)

Check

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ている脆弱性の影響を受けます。

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以降に移行してください。
2.6.x	脆弱性なし	脆弱性あり。3.12.3S以降に移行してください。
3.1.xS	脆弱性なし	脆弱性あり。3.12.3S以降に移行してください。
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以降に移行してください。
3.2.xSE	脆弱性なし	脆弱性あり。3.7.1E以降に移行してください。
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以降に移行してください。
3.3.xSE	脆弱性なし	脆弱性あり。3.7.1E以降に移行してください。
3.3.xSG	脆弱性なし	脆弱性あり。3.7.1E以降に移行してください。
3.3.xXO	脆弱性あり。3.7.0E以降に移行してください。	脆弱性あり。3.7.1E以降に移行してください。
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以降に移行してください。
3.4.xSG	脆弱性なし	脆弱性あり。3.7.1E以降に移行してください。

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以降に移行してください。
3.5.xE	脆弱性あり。3.7.0E以降に移行してください。	脆弱性あり。3.7.1E以降に移行してください。
3.6.xS	脆弱性なし	脆弱性あり。3.12.3S以降に移行してください。
3.6.xE	脆弱性あり。3.7.0E以降に移行してください。	脆弱性あり。3.7.1E以降に移行してください。
3.7.xS	脆弱性なし	脆弱性あり。3.12.3S以降に移行してください。
3.7.xE	脆弱性なし	3.7.1E
3.8.xS	脆弱性あり。3.10.5S以降に移行してください。	脆弱性あり。3.12.3S以降に移行してください。
3.9.xS	脆弱性あり。3.10.5S以降に移行してください。	脆弱性あり。3.12.3S以降に移行してください。
3.10.xS	3.10.5S	脆弱性あり。3.12.3S以降に移行してください。
3.11.xS	脆弱性あり。3.12.3S以降に移行してください。	脆弱性あり。3.12.3S以降に移行してください。
3.12.xS	3.12.3S	脆弱性あり。3.12.3S以降に移行してください。
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

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、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-20150325-tcpleak

改訂履歴

バージョン	説明	セクション	ステータス	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。