Cisco IOS Software and IOS XE Software TCP Packet Memory Leak Vulnerability

Advisory ID: cisco-sa-20150325-tcpleak

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

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。

Revision 1.1

Last Updated 2015 March 25 21:32 UTC (GMT)

For Public Release 2015 March 25 16:00 UTC (GMT)

目次

要約

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の攻撃者が該当デバイスのメモリ リークを引き起こし、最終的に該当デバイスのリロードが引き起こされる可能性があります。

この脆弱性は、TCP スリーウェイ ハンドシェイクの確立に使用される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、スリーウェイ ハンドシェイクを確立するときに、細工された TCP パケット シーケンスを送信することによって、この脆弱性を不正利用する可能性があります。この脆弱性を悪用することにより、攻撃者は該当デバイスのメモリ リークを発生させ、最終的に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無償のソフトウェア アップデートをリリースしました。このアド

バイザリは、次のリンクで確認できます。
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では、Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアに含まれる脆弱性に対応しています。個別の公開リンクは、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

脆弱性が認められる製品

この脆弱性の影響を受ける Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェアが稼働するシスコ デバイスには、この脆弱性が存在します。TCP ポートをリスニングするプロセスを持つ Cisco IOS または Cisco IOS XE ソフトウェアが稼働するシスコのデバイスは、潜在的に影響を受けます。Cisco IOS ソフトウェアには、TCP ポートをリスニングするよう設定できる複数のプロセスがあります。このように設定されたプロセスには、たとえば、HTTP、HTTPS、SSH、または Telnet があります。影響を受けるデバイスには、そのように設定されたその他のプロセスが存在し、TCP ポートをリスニングしている可能性があります。シスコ デバイスで TCP をリスニングするプロセスが有効かどうかを判断するために必要な設定は、設定されたプロセスに固有のものとなります。

Cisco IOS および Cisco IOS XE ソフトウェアが稼働する特定のデバイスでは、TCP ポートをリスニングす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 デバイスで、リスニングしているサービス宛てに送信された TCP パケットが処理されるかどうかを判断するには、デバイスにログインし、 **show tcp brief all** または **show control-plane host open-ports** コマンド ライン インターフェイス (CLI) コマンドのいずれかを実行します。出力に、TCP ポートでリスニングしているプロセスが表示される場合、そのデバイスは脆弱です。

次の例は、この脆弱性の影響を受ける Cisco IOS デバイスの表示例です。TCP ポート 80 および 22 をリスニングしているプロセスが存在するため、このデバイスは脆弱です。

```
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 brief all** および **show control-plane host open-ports** はプラットフォーム依存です。Cisco IOS または Cisco IOS XE ソフトウェアが稼働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 **show version** コマンドを実行してシステム バナーを表示させます。「Internetwork Operating System Software」、「Cisco IOS Software"」のようなテキストがシステム バナーに表示されていれば、デバイスで Cisco IOS ソフトウェアが稼働していることを示します。その後ろにイメージ名が括弧の間に表示され、続いて Cisco IOS ソフトウエア リリース番号とリリース名が表示されます。他のシスコ デバイスでは、**show version** コマンドがない場合や、表示が異なる場合があります。

次の例は、シスコ製品で Cisco IOS ソフトウェア リリース 15.2(4)M5 が稼働し、インストールされているイメージ名が C3900-UNIVERSALK9-M であることを示しています。

```
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_teamRouter> 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、ホワイト ペーパー「Cisco IOS and NX-OS Software Reference Guide」で確認できます。

脆弱性が認められない製品

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の攻撃者が該当デバイスのメモリ リークを引き起こし、最終的に該当デバイスのリロードが引き起こされる可能性があります。

この脆弱性は、TCP スリーウェイ ハンドシェイクの確立に使用される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、スリーウェイ ハンドシェイクを確立するときに、細工された TCP パケット シーケンスを送信することによって、この脆弱性を不正利用する可能性があります。この脆弱性を悪用することにより、攻撃者は該当デバイスのメモリ リークを発生させ、最終的に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、IPv4 パケットと IPv6 パケットの両方を使用して不正利用することができます。この脆弱性は、スリーウェイ 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ことがあります。細工された TCP パケット シーケンスは、デバイス上に構成されたインターフェイスの IPv4/IPv6 ユニキャスト アドレスを使用しており、TCP をリスニングしている ポート宛てである必要があります。

この脆弱性は該当デバイス宛てに送信される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。

脆弱な設定条件を満たすデバイスでは、巧妙に細工された TCP パケット シーケンスがこの脆弱性を引き起こす場合があります。インフラストラクチャの知識を持つ攻撃者は、この脆弱性を不正利用する特定の設定を持つ TCP パケットを作成できます。この脆弱性の不正利用に成功した場合、影響を受けたデバイス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。

脆弱性スコア詳細

シスコは本アドバイザリでの脆弱性に対し、Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。本セキュリティ アドバイザリでの CVSS スコアは、CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する組織の手助けとなる標準ベースの評価法です。

シスコでは、基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供しています。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、自身のネットワークにおける脆弱性の影響度を知ることができます。

シスコは次のリンクで CVSS に関する追加情報を提供しています。
http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

またシスコでは、各ネットワークにおける環境影響度を算出する CVSS 計算ツールを次のリンクで提供しています。
http://tools.cisco.com/security/center/cvssCalculator.x

CSCum94811 - Cisco IOS Software TCP Packet Memory Leak Vulnerability Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

この脆弱性の不正利用に成功した場合、該当デバイスのメモリ リークが引き起こされ、最終的にリロードが発生することがあります。この脆弱性が繰り返し不正利用されると、持続的なサービス拒否（DoS）状態に陥る可能性があります。

ソフトウェア バージョンおよび修正

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、起こりうる障害を判断し、それに対応できるアップグレード 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、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を判断するためのツールを提供しています。Cisco IOS ソフトウェア チェッカーを使用すると、お客様は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して、検索を開始します。
- **show version** コマンド出力を入力してツールで解析します。
- 以前に公開されたすべての Cisco Security Advisory、特定の公開内容、または 2015 年 3 月のすべてのバンドル公開内容を含めて、カスタマイズされた検索を作成します。

このツールにより、クエリされたソフトウェア リリースに影響を与える Cisco Security Advisory と、各 Cisco Security Advisory のすべての脆弱性を修正する最初のリリース（初回修正）を見つけることができます。このツールはさらに、表示された全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（総合初回修正）も分かります。Cisco IOS ソフトウェア チェッカーを使用するか、または以下のフィールドに Cisco IOS ソフトウェアのリリースを入力し、このバンドル公開に含まれているいずれかのアドバイザリの影響を受けるものがあるかどうかを判断してください。

（入力例：15.1(4)M2）

Cisco IOS XE ソフトウェア リリースの Cisco IOS ソフトウェア リリースへのマッピングについては、『Cisco IOS XE 2 リリース ノート』、『Cisco IOS XE 3S リリース ノート』、『Cisco IOS XE 3SG リリース ノート』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 Software Release	First Fixed Release	First Fixed Release for All Advisories in the March 2015 Cisco IOS Software Security Advisory Bundled Publication

2.5.x	Not vulnerable	Vulnerable; migrate to 3.12.3S or later.
2.6.x	Not vulnerable	Vulnerable; migrate to 3.12.3S or later.
3.1.xS	Not vulnerable	Vulnerable; migrate to 3.12.3S or later.
3.1.xSG	Not vulnerable	Not vulnerable
3.2.xS	Not vulnerable	Vulnerable; migrate to 3.12.3S or later.
3.2.xSE	Not vulnerable	Vulnerable; migrate to 3.7.1E or later.
3.2.xSG	Not vulnerable	Not vulnerable
3.2.xXO	Not vulnerable	Not vulnerable
3.2.xSQ	Not vulnerable	Not vulnerable
3.3.xS	Not vulnerable	Vulnerable; migrate to 3.12.3S or later.
3.3.xSE	Not vulnerable	Vulnerable; migrate to 3.7.1E or later.
3.3.xSG	Not vulnerable	Vulnerable; migrate to 3.7.1E or later.
3.3.xXO	Vulnerable; migrate to 3.7.0E or later.	Vulnerable; migrate to 3.7.1E or later.
3.3.xSQ	Not vulnerable	Not vulnerable
3.4.xS	Not vulnerable	Vulnerable; migrate to 3.12.3S or later.
3.4.xSG	Not vulnerable	Vulnerable; migrate to 3.7.1E or later.
3.4.xSQ	Not vulnerable	Not vulnerable
3.5.xS	Not vulnerable	Vulnerable; migrate to 3.12.3S or later.
3.5.xE	Vulnerable; migrate to 3.7.0E or later.	Vulnerable; migrate to 3.7.1E or later.
3.6.xS	Not vulnerable	Vulnerable; migrate to 3.12.3S or later.
3.6.xE	Vulnerable; migrate to 3.7.0E or later.	Vulnerable; migrate to 3.7.1E or later.

3.7.xS	Not vulnerable	Vulnerable; migrate to 3.12.3S or later.
3.7.xE	Not vulnerable	3.7.1E
3.8.xS	Vulnerable; migrate to 3.10.5S or later.	Vulnerable; migrate to 3.12.3S or later.
3.9.xS	Vulnerable; migrate to 3.10.5S or later.	Vulnerable; migrate to 3.12.3S or later.
3.10.xS	3.10.5S	Vulnerable; migrate to 3.12.3S or later.
3.11.xS	Vulnerable; migrate to 3.12.3S or later.	Vulnerable; migrate to 3.12.3S or later.
3.12.xS	3.12.3S	Vulnerable; migrate to 3.12.3S or later.
3.13.xS	Not vulnerable	3.13.2S
3.14.xS	Not vulnerable	Not vulnerable
3.15.xS	Not vulnerable	Not vulnerable

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』にて参照できます。
http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=37433

修正済みソフトウェアの入手

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 アップデートを提供しています。ソフトウェアの導入を行う前に、お客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境の特有の問題をご確認ください。

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、ご購入いただいたフィーチャ 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
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載の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。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、 Cisco.com の Software Navigator からアップグレードを入手することができます。 http://www.cisco.com/cisco/software/navigator.html

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、正しい処置についてのサポートを受けてください。

回避策や修正の効果は、使用している製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などに関するお客様の状況によって異なります。影響を受ける製品やリリースは多種多様であるため、回避策を実施する前に、対象ネットワークで適用する回避策または修正が最適であることを、お客様のサービス プロバイダーやサポート会社にご確認ください。

サービス契約をご利用でないお客様

シスコから製品を直接購入したもののシスコのサービス契約をご利用いただいていない場合、または、サードパーティ ベンダーから購入したものの修正済みソフトウェアを購入先から入手できない場合は、Cisco Technical Assistance Center（TAC）に連絡してアップグレード ソフトウェアを入手してください。

- +1 800 553 2447（北米からの無料通話）
- +1 408 526 7209（北米以外からの有料通話）
- Eメール：tac@cisco.com

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。サービス契約をご利用でないお客様は TAC に無償アップグレードをリクエストしてください。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、シスコ ワールドワイドお問い合わせ先（ http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html ）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）では、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とその公表は確認しておりません。

この脆弱性はサポート ケースの解決中に発見されたものです。

この通知のステータス：FINAL

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を示唆するものでもありません。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。またシスコはいつでも本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能

性があります。

情報配信

このアドバイザリは次のリンクにある Cisco Security に掲載されます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-tcpleak

また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の電子メールで配信されています。

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- fulldisclosure@seclists.org

本アドバイザリに関する今後の更新は Cisco.com に掲載されますが、メーリング リストで配信されるとは限りません。更新内容については、本アドバイザリの URL でご確認ください。

今後のドキュメントや関連コンテンツの入手手順については、 Security Vulnerability Policy ページの Receiving Security Vulnerability Information from Cisco を参照してください。

更新履歴

Revision 1.1	2015-March-25	Updated the First Fixed Release for All Advisories in the March 2015 Cisco IOS Software Security Advisory Bundled Publication table.
Revision 1.0	2015-March-25	Initial public release.

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関するサポート、およびシスコからセキュリティ情報を入手するための登録方法の詳細については、Cisco.com の http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html を参照してください。この Web ページには、Cisco Security Advisory に関してメディアが問い合わせる際の指示が掲載されています。すべての Cisco Security Advisory は、 http://www.cisco.com/go/psirt/ で確認することができます。
Cisco Security Advisories
Cisco Intrusion Prevention System Signatures
Cisco Applied Mitigation Bulletins
Cisco Security Blog
Cisco Event Response Pages
Cisco IntelliShield Alerts
Cisco Security Notices
Cisco Security Responses

Cisco Cyber Risk Reports
Cisco Security White Papers
Snort Rules