Cisco IOSソフトウェア TCP サービス拒否の脆弱性

High	**アドバイザリーID :** cisco-sa-20100812-tcp **初公開日 :** 2010-08-12 21:30 **バージョン 1.1 :** Final **CVSSスコア :** 7.8 **回避策 :** No Workarounds available **Cisco バグ ID :** CSCti18193	CVE-2010-2827

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 IOSÂ® ソフトウェア リリースは TCP 確立 フェーズの間にサービス拒否 （ DoS ）脆弱性から、15.1(2)T 影響を受けします。 脆弱性により萌芽期 TCP 接続は SYNRCVD または SYNSENT 状態を維持します可能性があります。 これらの状態の十分な萌芽期 TCP 接続はシステム リソースを消費し、影響を受けたデバイスが許可するか、またはデバイスへのあらゆる TCP ベースの遠隔管理 アクセスを含む新しい TCP 接続を、開始することを防ぐ可能性があります。

認証がこの脆弱性を不正利用するために必要となりません。 攻撃者はこの脆弱性を引き起こすために 3方向ハンドシェイクを完了する必要はありません; 従って、この脆弱性はスプーフィングされたパケットを使用して不正利用することができます。 この脆弱性は正常なネットワークトラフィックによって引き起こされるかもしれません。

Cisco はこの脆弱性に対処するために Cisco IOS ソフトウェア リリース 15.1(2)T0a をリリースしました。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100812-tcp で掲示されます。

該当製品

この脆弱性は Cisco IOS ソフトウェア リリースだけ 15.1(2)T 該当します。 他の Cisco IOS ソフトウェア リリースは影響を受けていません。 Cisco IOS XE ソフトウェア、Cisco IOS XR ソフトウェアおよび Cisco NX-OS ソフトウェアはこの脆弱性から影響を受けません。

脆弱性のある製品

Ciscoデバイスは Cisco IOS ソフトウェア リリース 15.1(2)T を実行しているとき脆弱です。 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。 "Internetwork Operating System Software"、"Cisco IOS Software" あるいはこれらに類似するシステム バナーによってデバイスで Cisco IOS ソフトウェアが稼働していることを確認できます。 その後ろにイメージ名が括弧の間に表示され、続いて "Version" と Cisco IOS ソフトウエア 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 C2800NM-ENTSERVICES-M のインストール済みイメージ名前と Cisco IOS ソフトウェア リリース 15.1(2)T を実行している Cisco製品を指定したものです:

```
Router#show version
Cisco IOS Software, 2800 Software (C2800NM-ENTSERVICES-M), Version 15.1(2)T,
    RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright Â©) 1986-2010 by Cisco Systems, Inc.
Compiled Mon 19-Jul-10 16:38 by prod_rel_team

<output truncated>
```

Cisco IOS ソフトウェア リリース 命名規則についてのその他の情報は白書で利用できます: Cisco IOSレファレンスガイド。

脆弱性を含んでいないことが確認された製品

他の Cisco IOS ソフトウェア バージョン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

TCP はパケット交換網環境の信頼できるデータ転送 サービスを提供します。 TCP はトランスポート層（OSI 参照モデルにの 4）層対応します。 TCP が提供するサービスの間でストリーム データ転送、信頼性、効率的なフロー制御、全二重モードでの動作および多重化はあります。

TCP 接続が Cisco IOSソフトウェアで終わるとき、伝達 コントロール ブロック（TCB）割り当てられます。 すべての割り当てられた TCBs、関連する TCPポート数および TCP 状態は **show tcp 要約**の出力で**すべての** Command Line Interface （CLI）コマンド 表示する。

Cisco IOS ソフトウェア バージョン 15.1(2)T は萌芽期 TCP 接続がそれ以上の TCP 状態移行なしで SYNRCVD または SYNSENT 状態を維持します可能性がある脆弱性が含まれています。 **show tcp** の出力を検査して TCP セッションがこれらの状態の 1 つに残る場合複数回が示す**すべての**コマンドを**報告して下さい**。

終えられるか、またはデバイスから起こされるこの脆弱性は TCPトラフィックによってだけ引き起こされます。 トランジットトラフィックはこの脆弱性を引き起こしません。

ルータに出入する接続は両方ともこの脆弱性を引き起こす可能性があります。 ルータへの接続の例はまだデバイスを ping できるデバイスへの TELNET または SSH 接続を確立しませんこと。 たとえば、管理者はまだデバイスを ping してできるかもしれませんデバイスへの Telnet か SSH 接続を確立しないために。 CLI プロンプトからのリモートデバイスへの Telnet か SSH 接続を試みる管理者はハングアップセッションおよび「試みることに < IP アドレス出会います|ホスト名 >...」 プロンプトで発行します。 ルータで開始されるか、または終わる接続はソケット テーブルから **clear tcp tcb 0x<address>** コマンドで関連する TCB のクリアによって取除くことができます。

デバイスは CLI コマンド **debug ip tcp transactions** の出力を検査している場合、表示する エラーメッセージ 脆弱である可能性があります： `<port number>` か： `<port number>`。

デバイスはまたすべての CLI コマンドが状態 SYNRCVD か SYNSENT の多くの TCBs を示す反復的な show tcp 要約から出力された場合脆弱である可能性があります。

次の例は TCP SYNRCVD 状態で複数 HTTP、SSH および Telnetセッションを備えているデバイスを示したものです:

```
Router#show version
Cisco IOS Software, 2800 Software (C2800NM-ENTSERVICES-M), Version 15.1(2)T,
    RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright Â©) 1986-2010 by Cisco Systems, Inc.
Compiled Mon 19-Jul-10 16:38 by prod_rel_team

<output truncated>
```

どの TCP セッションでも **clear tcp tcb 0x *<address>*** が付いている関連する TCB のクリアによってクリアすることができます。 また管理者は **clear tcp tcb の**発行によってすべての TCBs をすぐにクリアできます*。

注: これはすべてのアクティブおよびハングさせた TCP 接続をクリアします。

この脆弱性は Cisco バグ ID **CSCti18193**（登録ユーザのみ）で文書化されています。 この脆弱性よくある脆弱性および公開（CVE）ID CVE-2010-2827 は割り当てられました。

TCP アプリケーション特有の情報は以降のセクションで提供されます:

Telnet および SSH

Telnet は Cisco IOSデバイスで明示的にディセーブルにすることができません。 **トランスポート入力を**設定して脆弱 な デバイスの VTY 行の**どれも**防ぎません TCPポート 23 で不正利用されることを。 ただし、Cisco IOS SSH サーバ 機能がデバイスで設定されれば、**トランスポート入力はどれも**デバイスが TCPポート 22 で不正利用されることを防ぎません。

VTY アクセスコントロール アクセス・コントロール・リストの設定は脆弱性がスプーフィングされたIP 送信元アドレスを使用して不正利用することができるので部分的にこの脆弱性を軽減できます。

Border Gateway Protocol（BGP）

ボーダー ゲートウェイ プロトコル（BGP）で設定されるルータは一般化された Time To Live（TTL）セキュリティ機構（GTSM）機能の使用によって更に保護することができます。 GTSM はユーザが送信元 および 宛先アドレス間のパケットの期待された TTL を設定することを可能にします。 GTSM チェック失敗するパケットは TCP処理が発生する前に廃棄されます、攻撃者は BGP によってこの脆弱性を不正利用することを防ぐ。 GTSM はコマンド TTL **セキュリティ ホップ**と設定されます。

BGP の保護のより詳しい 情報は[エンタープライズのための Border Gateway Protocol（BGP）保護](#)で見つけることができます。

BGP のための TCP MD5認証はこの脆弱性が不正利用されることを防ぎません。

セキュリティ侵害の痕跡

回避策

この脆弱性を軽減する唯一の完全な回避策はこの操作が実行可能である場合、デバイスを脆弱にする特定の機能をディセーブルにすることです。

正当 な デバイスだけ影響を受けたデバイスに接続するようにすることはこの脆弱性への公開の制限を助けます。 次のコントロール プレーン ポリシングおよび更に詳しい情報についてはインフラストラクチャ アクセス リスト サブセクションの設定を参照して下さい。 TCP 3 ウェイ ハンドシェイクが必要とならないので効果を高める、軽減はネットワークエッジのアンチスプーフィング手段と結合する必要があります。

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/content/CiscoAppliedMitigationBulletin/cisco-amb-20100812-tcp。

Cisco IOS デバイスの強化ガイド

Cisco IOSデバイスを堅くする Cisco ガイドは TCP 状態操作脆弱性を軽減する多くの有用な手法の例を提供します。 これには次のものがあります。

- Infrastructure Access Control List（iACL; インフラストラクチャ アクセス コントロール リスト）

- Receive Access Control List （ rACL ）
- アクセス コントロール リスト（ ACL ）中継（ tACL ）
- VTY アクセス コントロール リスト（ ACL ）
- コントロール プレーン ポリシング（ CoPP ）
- コントロール プレーン 保護（ CPPr ）

これらのトピックに関する詳細については、Cisco IOSデバイスを堅くするために Cisco ガイドを参照して下さい。

CoPP

TCP サービスを提供する必要があるデバイスの場合管理者は信頼できないソースからの TCPトラフィックをブロックするのに影響を受けたデバイスに向かう CoPP を使用できます。 Cisco IOS ソフトウェア リリース 12.0S、12.2SX、12.2S、12.3T、12.4、および 12.4T は、CoPP 機能をサポートしています。 CoPP はデバイスで管理および制御平面を保護し、明示的に 既存 の セキュリティポリシーおよびコンフィギュレーションに従ってインフラストラクチャ デバイスに送信 される承認されたトラフィックだけ許可することによって直接インフラストラクチャ不正侵入のリスクおよび効果を最小に するために設定されるかもしれません。 次の例は特定のネットワークコンフィギュレーションに適応させることができます:

```
Router#show version
Cisco IOS Software, 2800 Software (C2800NM-ENTSERVICES-M), Version 15.1(2)T,
    RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright Â©) 1986-2010 by Cisco Systems, Inc.
Compiled Mon 19-Jul-10 16:38 by prod_rel_team

<output truncated>
```

警告： この脆弱性を不正利用するために TCP 3 ウェイ ハンドシェイクが必要とならないので信頼された IP アドレスからのこれらのポートにアクセス コントロール リスト（ ACL ）をその割り当て通信敗北させる可能性がある送信側の IP アドレスをスプーフィングすることは可能性のあるです。

CoPP 先行する例では、「拒否」操作を一致するパケットは policy-map ドロップする 機能から（ 示されていない ）影響を受けないが policy-map 「ドロップする」機能によって廃棄されるこれらのパケットの「割り当て」アクションの結果を用いる潜在的なエクスプロイト パケット一致する アクセス制御エントリ（ ACE ）その。 CoPP 機能の設定および使用のその他の情報はコントロール プレーン ポリシング 実装 最良 の 方法およびコントロール プレーン ポリシングで見つけることができます。

iACLs の設定

ネットワークを通過する頻繁にトラフィックをブロックすることは困難であるが、決してインフラストラクチャ デバイスを目標とし、ネットワークのボーダーでそのトラフィックをブロックするようにするべきではないトラフィックが識別することは可能性のあるです。 インフラストラクチャ ACL はネットワーク セキュリティのベスト プラクティスと考えられており、ここでの特定

の脆弱性の回避策としてだけでなく、優れたネットワーク セキュリティへの長期的な付加機能として考慮する必要があります。 コアを保護する白書: インフラストラクチャ 保護はアクセス コントロール リスト（ACL）インフラストラクチャ 保護 ACL のためのガイドラインおよび推奨される配備手法を示します。

BGP 考慮事項

GTSM はどの TCP処理でも発生する前に GTSM を設定される TTL チェックをパスしないデバイスから起こすパケットが廃棄されるので BGP ポートによってこの脆弱性の不正利用を防ぐのを助けることができます。 GTSM の情報に関しては TTL 保安検査および BGP 存続可能時間 保安検査用の BGPサポートを参照して下さい。

組み込みイベント マネージャ（EEM）

脆弱 な Cisco IOSデバイスで Cisco IOS Embedded Event Manager（EEM）ポリシーが Tool Command Language（Tcl）に基づいているこの脆弱性によって引き起こされるハングさせるか、拡張されるか、または不明確な TCP 接続を識別し、検出するのに使用することができます。 ポリシーは管理者が Cisco IOSデバイスの TCP 接続を監視することを可能にします。 Cisco IOS EEM がこの脆弱性の潜在的な不正利用を検出するとき、ポリシーは syslog メッセージか TCP 接続をクリアするために簡易 ネットワーク 管理 プロトコル（SNMP）トラップの送信によって応答を引き起こすことができます。 この文書で提供されるポリシーの例は定義された間隔で 2 つのコマンドからの出力を監察し、解析する Tcl スクリプトにモニタ しきい値が設定値に達する、TCP 接続をリセットできます基づいていますとき、表示し syslog メッセージを。

Tcl スクリプトは Cisco で向こうダウンロード可能です: 次のリンク http://forums.cisco.com/eforum/servlet/EEM?page=eem&fn=script&scriptId=2041 の組み込みイベント マネージャ（EEM）スクリプトを書くコミュニティ、およびデバイス 設定 例は下記に提供されます。

```
Router#show version
Cisco IOS Software, 2800 Software (C2800NM-ENTSERVICES-M), Version 15.1(2)T,
    RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright Â©) 1986-2010 by Cisco Systems, Inc.
Compiled Mon 19-Jul-10 16:38 by prod_rel_team

<output truncated>
```

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際には、http://www.cisco.com/go/psirt およびそれ以降のアドバイザリも参照して、起こりうる障害と完全なアップグレード ソリューションを判断してください

いずれの場合も、アップグレードする機器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しいリリースで引き続き適切にサポートされていることの確認を十

分に行ってください。 情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

Cisco IOS ソフトウェアの表（下掲）の各行には、Cisco IOS のリリース トレインが記載されています。 リリース トレインが脆弱である場合、最も早い可能性のある リリースは表の「最初修正済みリリース」カラムに修正が含まれている（それぞれのための入手可能予想日と共に、該当する場合）リストされています。 「推奨リリース」列には、このアドバイザリが作成された時点で発表されているすべての脆弱性の修正を含むリリースが記載されます。 特定の列に記されているリリースよりも古い（第 1 修正済みリリースより古い）トレインに含まれるリリースが稼働しているデバイスは脆弱であることが確認されています。 表の「推奨リリース」列に記載されているリリース、またはそれよりも新しいリリースにアップグレードすることを推奨します。

メジャー リリース	**修正済みリリースの入手可能性**
該当する 12.x ベースのリリース	**First Fixed Release（修正された最初のリリース）**
12.0 - 12.4	12.0 ～ 12.4 基づいたリリースは影響を受けていません
該当する 15.0 ベースのリリース	**First Fixed Release（修正された最初のリリース）**
15.0	該当する 15.0 基づいたリリースがありません
該当する 15.1 ベースのリリース	**First Fixed Release（修正された最初のリリース）**
15.1T	15.1(2)T0a 15.1(2)T1; 20-AUG-2010 で利用可能 15.1(2)T 以前のリリースは脆弱ではないです。 脆弱性はリリース 15.1(2)T0a で最初に解決されます。

不正利用事例と公式発表

Cisco PSIRT はこのアドバイザリに記載される脆弱性の公示か不正利用に気づいていません。

この脆弱性は、お客様 によって Cisco に報告されました。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100812-tcp

改訂履歴

リビジョン 1.0	2010-August-12	Initial public release.

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。