Cisco IOS cTCP サービス拒否の脆弱性

High	**アドバイザリーID :** cisco-sa-20090325-ctcp **初公開日 :** 2009-03-25 16:00 **バージョン 1.1 :** Final **CVSSスコア :** 7.8 **回避策 :** No Workarounds available **Cisco バグ ID :** CSCsr16693 CSCsu21828	CVE-2009-0635

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

一連の TCP パケットにより Cisco トンネリング 制御プロトコル（cTCP）カプセル化 機能で Easy VPN サーバで設定されるサービス拒否 （DoS）状態 IOSデバイスを on Cisco 引き起こすかもしれません。 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。 対応策は見つかりません; ただし、IPSec NAT 走査（NAT-T）機能は代替として使用することができます。

このアドバイザリは 325-ctcp で掲示されます。

注: 2009 年 3月 25 日、Cisco IOS セキュリティ アドバイザリによって組み込まれる書は 8 つのセキュリティ アドバイザリが含まれています。 アドバイザリすべては Cisco IOSソフトウェアの脆弱性に対処します。 各アドバイザリはリリースをリストしますアドバイザリの脆弱性を解決する。

各ドキュメントへのリンクは次のとおりです。

- Cisco IOS cTCP サービス拒否の脆弱性
  325-ctcp

- Cisco IOSソフトウェア倍数は IP ソケット脆弱性を特色にします
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ip

- Cisco IOSソフトウェア モバイル IP およびモービル IPv6 脆弱性

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-mobileip

- Cisco IOSソフトウェア Secure Copy（SCP） 特権 拡大脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-scp

- Cisco IOSソフトウェア Session Initiation Protocol（SIP） サービス拒否の脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-sip

- Cisco IOSソフトウェア複数の機能によって細工 される TCP シーケンス脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-tcp

- Cisco IOSソフトウェア複数の機能 巧妙に細工された UDP パケットの脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-udp

- Cisco IOSソフトウェア WebVPN および SSLVPN 脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-webvpn

該当製品

脆弱性のある製品

バージョン 12.4(9)T または それ 以降を実行し、Cisco EZVPN サーバのトンネリング 制御プロトコル（cTCP）カプセル化のために設定される Cisco IOSデバイスは脆弱です。

注: cTCP カプセル化 機能は Cisco IOSバージョン 12.4(9)T で導入されました。 cTCP カプセル化 機能はデフォルトでディセーブルにされます。 EzVPN クライアントのために設定される Cisco IOSデバイスはこの脆弱性から影響を受けません。 EZVPN サーバで設定されるデバイスだけ脆弱です。

Easy VPN のための cTCP カプセル化 機能を設定するために、グローバル コンフィギュレーション モードで**暗号 ctcp** コマンドを使用して下さい。 デバイスが**暗号 ctcp ポート <port>** コマンドでを受信することオプションでポート番号を規定できます。 10 までの番号は設定し、ポート値は 1 ～ 65535 のどれである場合もあります。 Port キーワードが設定されない場合、デフォルトポート番号は 10000 です。 次の例では、Cisco IOSデバイスはポート 10000 の

cTCP メッセージを聞き取るために設定されます。

```
crypto ctcp port 10000
```

注: Port キーワードは EZVPN サーバとして機能する Cisco IOSデバイスでだけ設定されます。

デバイスに Cisco製品、ログインで動作する Cisco IOSソフトウェアのバージョンを判別し、システムバナーを表示する **show version コマンドを**発行するため。 Cisco IOS ソフトウェアは「Internetwork Operating System Software」または単に「IOS」と表示されます。 出力次の行で、イメージ名は「バージョンに」先行しているかっこと IOSリリース名の間で表示する。 その他の Cisco デバイスには **show version** コマンドがないか、異なる出力が返されます。

次の例は C2500-IS-L 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 12.3(26) を実行する Cisco製品を指定したものです:

```
    Router#show version
    Cisco Internetwork Operating System Software
    IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE (fc2)
    Technical Support: http://www.cisco.com/techsupport
    Copyright (c) 1986-2008 by cisco Systems, Inc.
    Compiled Mon 17-Mar-08 14:39 by dchih

  <output truncated>
```

次 の 例は C1841-ADVENTERPRISEK9-M のイメージ名と Cisco IOS ソフトウェア リリース 12.4(20)T を実行する製品を示します:

```
    Router#show version
    Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE
SOFTWARE (fc3)
    Technical Support: http://www.cisco.com/techsupport
    Copyright (c) 1986-2008 by Cisco Systems, Inc.
    Compiled Thu 10-Jul-08 20:25 by prod_rel_team

  <output truncated>
```

Cisco IOSリリース命名規則のその他の情報は「白書と資格を与えられる文書で見つけることができます: http://www.cisco.com/warp/public/620/1.html で利用可能である 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

cTCP のために設定されない Cisco IOSデバイスはこの脆弱性から影響を受けません。 Cisco ASA および Cisco VPN 3000 シリーズ コンセントレータは脆弱ではないです。 EzVPN クライアントで設定される Cisco IOSデバイスはこの脆弱性から影響を受けません。 Cisco VPN Client は脆弱ではないです。 Cisco IOS XR および Cisco IOS XE 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 トンネリング 制御プロトコル（cTCP）機能は標準 IPSec が既存のファイアウォール ルールへの修正なしでは透過的に機能しない環境で動作する Easy VPN Remote デバイスによって使用されます。 cTCP トラフィックは実際に TCPトラフィックです。 Cisco IOS cTCP パケットは TCP に送信されているインターネット キー エクスチェンジ（IKE）または Encapsulating Security Payload（ESP）パケットです。

脆弱性はにどの一連の TCP パケットによりメモリを使い果たすために cTCP カプセル化 機能で Easy VPN Server で設定される Cisco IOSデバイスを引き起こすかもしれないかあります。 この脆弱性は Cisco バグ ID CSCsr16693（登録ユーザのみ）および CSCsu21828（登録ユーザのみ）で文書化されています; そしてよくある脆弱性および公開（CVE）識別子 CVE-2009-0635 を割り当てられました。

セキュリティ侵害の痕跡

回避策

対応策は見つかりません。

代替として、IPSec NAT 走査（NAT-T）機能は使用することができます。 IPSec NAT-T 機能は NAT と IPSec の間で多くの既知非互換性を当たることによってネットワークのネットワーク アドレス変換（NAT）またはポート アドレス変換 （PAT）ポイントを移動するために IP Security（IPSec）トラフィックのためのサポートを導入します。

注: NAT-T 機能は Cisco IOSバージョン 12.2(13)T で導入されました。

NAT トラバーサルは、VPN デバイスによって自動的に検出される機能です。 Cisco IOS Release 12.2(13)T および それ 以降を実行するルータのためのコンフィギュレーションのステップがありません。 VPN デバイスが両方とも可能な NAT-T である場合 NAT 走査は自動検出され、オート・ネゴシエートされます。

注: NAT-T を有効に するとき、Cisco IOSデバイスは自動的に IPSec すべての使用可能なインターフェイスの UDP ポート 4500 をオープンにします。

注意： NAT-T をサポートすることを IPSec over UDP VPN ソフトウェアクライアントが on Cisco 可能にする必要がある場合もあることに注意して下さい。 さらに、インターネット キー エクスチェンジ（IKE）のための UDP ポート 500 および NAT-T のための UDP ポート 4500 を許可するファイアウォール ルールを変更する必要がある場合もあります。

NAT-T に関する詳細については、白書をで参照して下さい:

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_ipsec_nat_transp.html

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。

325-ctcp

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。 特定のリリース トレインに脆弱性がある場合は、修正を含む最初のリリース（および、それぞれの予想提供日）が表の「第 1 修正済みリリース」列に記載されます。 「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**	
Affected 12.0-Based Releases	**First Fixed Release（修正された最初のリリース）**	**推奨リリース**
該当する 12.0 ベースのリリースはありません。		
Affected 12.1-Based Releases	**First Fixed Release（修正された最初のリリース）**	**推奨リリース**
該当する 12.1 ベースのリリースはありません。		
Affected 12.2-Based Releases	**First Fixed Release（修正された最初のリリース）**	**推奨リリース**
該当する 12.2 基づいたリリースがありません		
Affected 12.3-Based Releases	**First Fixed Release（修正された最初のリリース）**	**推奨リリース**
該当する 12.3 ベースのリリースはありません。		

Affected 12.4-Based Releases	First Fixed Release（修正された最初のリリース）	推奨リリース
12.4	脆弱性なし	
12.4JA	脆弱性なし	
12.4JDA	脆弱性なし	
12.4JK	脆弱性なし	
12.4JL	脆弱性なし	
12.4JMA	脆弱性なし	
12.4JMB	脆弱性なし	
12.4JX	脆弱性なし	
12.4MD	脆弱性なし	
12.4MR	脆弱性なし	
12.4SW	脆弱性なし	
12.4T	12.4(20)T2 12.4(15)T9; 29-APR-2009 で利用可能	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XA	脆弱性なし	
12.4XB	脆弱性なし	
12.4XC	脆弱性なし	
12.4XD	脆弱性なし	
12.4XE	脆弱性なし	
12.4XF	脆弱性なし	
12.4XG	脆弱性なし	
12.4XJ	脆弱性なし	
12.4XK	脆弱性なし	
12.4XL	脆弱性なし	
12.4XM	脆弱性なし	
12.4XN	脆弱性なし	
12.4XP	脆弱性なし	
12.4XQ	脆弱性なし	
12.4XR	脆弱性なし	
12.4XT	脆弱性なし	
12.4XV	脆弱性なし	
12.4XW	脆弱性なし	
12.4XY	脆弱性なし	
12.4XZ	12.4(15)XZ2	12.4(15)XZ2
12.4YA	12.4(20)YA2	12.4(20)YA3
12.4YB	脆弱性なし	

12.4YD	脆弱性なし	

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。

この脆弱性はテクニカルサポート サービス 要求の解決の間に発見されました。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ctcp

改訂履歴

リビジョン 1.1	2009-June-25	March/09 によって結合される修正済みソフトウェア 表への取除かれた参照。
リビジョン 1.0	2009-March-25	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。