Cisco Security Advisory: Cisco IOS cTCP Denial of Service Vulnerability

Advisory ID: cisco-sa-20090325-ctcp

http://www.cisco.com/warp/public/707/cisco-sa-20090325-ctcp.shtml

本翻訳は、原文の機械翻訳後に技術者が簡易レビューをしたものです。 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 2009 June 25 2200 UTC (GMT)

For Public Release 2009 March 25 1600 UTC (GMT)

目次

要約

Cisco Tunneling Control Protocol (cTCP)カプセル化機能を利用する Easy VPN サーバとして設定された Cisco IOSデバイスにおいて、連続した TCPパケットがサービス拒絶(DoS)状態を引き起こす可能性があります。Ciscoはこの脆弱性に対処する無償のソフトアップデートをリリースしました。回避策はありません。ただし、IPSec NAT Traversal (NAT-T) 機能を代替として使用することが可能です。

このアドバイザリは次のリンクに掲載されます:
http://www.cisco.com/JP/support/public/ht/security/106/1065614/cisco-sa-20090325-ctcp-j.shtml

注:2009年 3月 25日のIOSアドバイザリバンドル公開には 8つの Security Advisory が含まれていま

す。それらは全て Cisco IOS ソフトウェアの脆弱性に対処するものです。各アドバイザリには、そのアドバイザリで記述された脆弱性を解決するリリースを記載しています。個々の公開リンクは下記に掲載されています:

- Cisco IOS cTCP Denial of Service Vulnerability
  http://www.cisco.com/JP/support/public/ht/security/106/1065614/cisco-sa-20090325-ctcp-j.shtml

- Cisco IOS Software Multiple Features IP Sockets Vulnerability
  http://www.cisco.com/JP/support/public/ht/security/106/1065617/cisco-sa-20090325-ip-j.shtml

- Cisco IOS Software Mobile IP and Mobile IPv6 Vulnerabilities
  http://www.cisco.com/JP/support/public/ht/security/106/1065612/cisco-sa-20090325-mobileip-j.shtml

- Cisco IOS Software Secure Copy Privilege Escalation Vulnerability
  http://www.cisco.com/JP/support/public/ht/security/106/1065615/cisco-sa-20090325-scp-j.shtml

- Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability
  http://www.cisco.com/JP/support/public/ht/security/106/1065619/cisco-sa-20090325-sip-j.shtml

- Cisco IOS Software Multiple Features Crafted TCP Sequence Vulnerability
  http://www.cisco.com/JP/support/public/ht/security/106/1065621/cisco-sa-20090325-tcp-j.shtml

- Cisco IOS Software Multiple Features Crafted UDP Packet Vulnerability
  http://www.cisco.com/JP/support/public/ht/security/106/1065622/cisco-sa-20090325-udp-j.shtml

- Cisco IOS Software WebVPN and SSLVPN Vulnerabilities
  http://www.cisco.com/JP/support/public/ht/security/106/1065618/cisco-sa-20090325-webvpn-j.shtml

該当製品

脆弱性のある製品

12.4(9)T またはそれ以降のソフトウェアバージョンで動作しており、Cisco Tunneling Control Protocol (cTCP) カプセル化を利用する EZVPN サーバとなっている Cisco IOS デバイスには脆弱性があります。

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無効となっています。EZVPN クライアントとして動作している Cisco IOS デバイスはこの脆弱性の影響を受けません。EZVPN サーバとして設定されたデバイスが脆弱性の対象となります。

Easy VPN で cTCP カプセル化機能を利用する場合には、グローバルコンフィギュレーションモードで **crypto ctcp** コマンドを使用します。デバイスはオプションとして **crypto ctcp port <port>** コマンドで cTCP パケットを受信するポート番号を指定することが可能です。10件までの設定が可能であり、指定可能なポート番号は1から65535までの範囲内となります。port を指定しない場合、デフォルトのポート番号には10000が用いられます。例として Cisco IOS デバイスが cTCP メッセージの受信ポートを10000とする場合には以下のように設定します。

```
crypto ctcp port 10000
```

注: port キーワードは EZVPN サーバとして動作している Cisco IOS デバイスにおいてのみ設定が可能です。

Cisco 製品で稼動中の Cisco IOS ソフトウェア リリースを確認するには、機器にログインし **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。Cisco IOS ソフトウェアは、"Internetwork Operating System Software" もしくは "Cisco IOS Software" と表示されます。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 Cisco 機器では、show version コマンドがない場合や、異なる表示をする場合があります。

以下の例では、Cisco 製品にて、IOSリリース 12.3(26) が稼動し、そのイメージ名が C2500-IS-L であることを示しています:

```
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>
```

次の例では、Cisco IOS ソフトウェアリリース 12.4(20)T が稼働し、イメージ名が C1841-ADVENTERPRISEK9-M であることを示しています:

```
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 ソフトウエアのリリース命名規則の追加情報は以下のリンクの "White Paper: Cisco IOS Reference Guide"で確認できます: http://www.cisco.com/warp/public/620/1.html

脆弱性が存在しない製品

cTCP の設定がなされていない Cisco IOS デバイスはこの脆弱性の影響を受けません。Cisco ASA および Cisco VPN 3000 series Concentrator はこの脆弱性に該当しません。EZVPN クライ

アントとして設定された Cisco IOS デバイスはこの脆弱性の影響を受けません。Cisco VPN Client はこの脆弱性に該当しません。Cisco IOS-XR および Cisco IOS-XE 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本アドバイザリーの影響を受けるものは現在確認されていません。

詳細

Cisco Tunneling Control Protocol (cTCP) 機能は、既存のファイアウォール・ルールによって一般的な IPSec トラフィックが遮断される環境で運用されている Easy VPN リモートデバイスで利用されます。 cTCP のトラフィックは TCP のトラフィックです。 Cisco IOS の cTCP パケットは、Internet Key Exchange (IKE) または Encapsulating Security Payload (ESP) パケットが TCP によってカプセル化されたものです。

この脆弱性によって、cTCP カプセル化機能を利用する Easy VPN サーバとして動作している Cisco IOS デバイスでは、連続した TCP パケットが送信されることによってメモリが大量に消費される可能性があります。この脆弱性は Cisco Bug 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。また、Common Vulnerabilities and Exposures (CVE) ID CVE-2009-0635 が割り当てられています。

脆弱性スコア詳細

Cisco はこのアドバイザリでの脆弱性に対して Common Vulnerability Scoring System (CVSS)に基づいたスコアを提供しています。このセキュリティアドバイザリでの CVSSスコアは CVSS version 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手助けとなる標準ベースの評価法です。Cisco は基本評価 (Base Score) および現状評価スコア (Temporal Score) を提供いたします。お客様はこれらを用いて環境評価スコア (Environmental Score) を算出し、個々のネットワークにおける脆弱性の影響度を導き出すことができます。

Cisco は以下の URL にて CVSS に関する FAQ を提供しています。

http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html また Cisco は個々のネットワークにおける環境影響度を算出する CVSS 計算ツールを以下の URL にて提供しています。

http://intellishield.cisco.com/security/alertmanager/cvss

CSCsr16693 - cTCP server may crash when processing a series of TCP packets **Calculate the environmental score of**					
CVSS Base Score - **7.8**					
Access	Access Comple	Authentication	Confidentiality	Integrity	Availability

Vector	xity		Impact	Impact	Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCsu21828 - Cisco IOS Device may crash with cTCP enabled **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より、Cisco IOS デバイスはメモリを大量に消費する可能性があります。不正利用が繰り返された場合にはサービス拒否 (DoS) の状態になることがあります。

ソフトウエアバージョン及び修正

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、本アドバイザリ以降に公開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。 情報が不明確な場合は、Cisco Technical Assistance Center (TAC) もしくは契約している保守会社にお問い合せください。Cisco IOS ソフトウェアテーブル(下記)の各行は Cisco IOS のリリーストレインを示します。 あるリリーストレインが脆弱である場合、修正を含む最初のリリースは、 表の "First Fixed Release" 列に示されます(入手可能予想日が示される場合もあります)。 "Recommended Release" 列は、このアドバイ

ザリの公開時点において 公開済みである全ての脆弱性についての修正を含むリリースを示します。 実行しているリリースが、そのトレインで "First Fixed Release" 以前のものである 機器は脆弱であることが知られています。 Cisco はテーブルの "Recommended Releases" 列のリリース、またはそれ以降のリリースにアップグレードすることを推奨します。

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Releases	First Fixed Release	Recommended Release
There are no affected 12.0 based releases		
Affected 12.1-Based Releases	First Fixed Release	Recommended Release
There are no affected 12.1 based releases		
Affected 12.2-Based Releases	First Fixed Release	Recommended Release
There are no affected 12.2 based releases		
Affected 12.3-Based Releases	First Fixed Release	Recommended Release
There are no affected 12.3 based releases		
Affected 12.4-Based Releases	First Fixed Release	Recommended Release
	Not Vulnerable	
	Not Vulnerable	
	Not Vulnerable	
	Not Vulnerable	
	Not Vulnerable	
	Not Vulnerable	
	Not Vulnerable	
	Not Vulnerable	
	Not Vulnerable	
	Not Vulnerable	
	Not Vulnerable	
	Not Vulnerable	
	12.4(20)T2 12.4(15)T9; Available on 29-APR-2009	12.4(22)T1 12.4(15)T9; Available on 29-APR-2009
	Not Vulnerable	
	Not Vulnerable	
	Not Vulnerable	
	Not Vulnerable	
	Not Vulnerable	
	Not Vulnerable	

	Not Vulnerable	
	Not Vulnerable	
	Not Vulnerable	
	Not Vulnerable	
	Not Vulnerable	
	Not Vulnerable	
	Not Vulnerable	
	Not Vulnerable	
	Not Vulnerable	
	Not Vulnerable	
	Not Vulnerable	
	Not Vulnerable	
	Not Vulnerable	
	Not Vulnerable	
	12.4(15)XZ2	12.4(15)XZ2
	12.4(20)YA2	12.4(20)YA3
	Not Vulnerable	
	Not Vulnerable	

回避策

cTCP 機能を用いている場合、回避策はありません。

cTCP の代替として、IPSec NAT Traversal (NAT-T) 機能を使用することができます。IPSec NAT-T 機能は、ネットワーク内に Network Address Translation (NAT) あるいは Port Address Translation (PAT) を用いたポイントが存在する場合でも IP Security (IPSec) のトラフィックを通過可能とするために、NAT と IPSec を併用するにあたって存在する多くの不整合を回避することを可能とするものです。

注: NAT-T 機能は Cisco IOS バージョン 12.2(13)T で導入されています。

NAT Traversal 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 およびそれ以降が動作しているルータでは、特に設定を必要としません。VPN デバイスが共に NAT-T を利用可能である場合、NAT Traversal は自動的に検出され、自動的にネゴシエートされます。

注: NAT-T が有効化された場合、Cisco IOS デバイスでは IPsec が有効化されているすべてのインターフェイスにおいて UDP のポート4500が Open となります。

注意: Cisco VPN Software Client では、NAT-T をサポートするために IPSec over UDP を有効にする必要があります。また、Internet Key Exchange (IKE) に用いる UDP のポート500 及び NAT-T に用いる UDP のポート4500 での通信を許可するようファイアウォール・ルールを変更する必要があります。

NAT-T に関する詳細につきましては、以下の whitepaper を参照して下さい:

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

ネットワーク内の Cisco 機器に適用可能な他の緩和策は、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://www.cisco.com/warp/public/707/cisco-amb-20090325-ctcp.shtml

修正済みソフトウェアの入手

Cisco はこれらの脆弱性に対応するための無償ソフトウェア 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ーセットの互換性および お客様のネットワーク環境に特有の問題に関してご確認下さい。

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ー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 Cisco のソフトウェア ライセンスの条項または、 Cisco.com Downloads の http://www.cisco.com/public/sw-center/sw-usingswc.shtml に説明のあるその他の条項に従うことに同意したことになります。

ソフトウェアのアップグレードに関し、"psirt@cisco.com" もしくは "security-alert@cisco.com" に お問い合わせいただくことはご遠慮ください。

サービス契約をお持ちのお客様

契約をお持ちのお客様は、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 のワールドワイドウェブサイト上の ソフトウェアセンター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

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 Cisco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、本脆弱性に関する適切な処置について指示と支援を受けてください。 回避策の効果は、使用製品、ネットワークトポロジー、トラフィックの性質や 組織の目的などのお客様の状況に依存します。影響製品が多種多様であるため、 回避策を実際に展開する前に、対象とするネットワークで適用する回避策が最適であるか、 お客様のサービスプロバイダーやサポート組織にご相談ください。

サービス契約をご利用でないお客様

Cisco から直接購入したが Cisco のサービス契約をご利用いただいていない場合、 また、サードパーティ ベンダーから購入したが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を入手してください。 TAC の連絡先は次のとおりです。

- +1 800 553 2447 (北米内からのフリー ダイヤル)
- +1 408 526 7209 (北米以外からの有料通話)
- 電子メール： tac@cisco.com

無料アップグレードの対象であることをご証明いただくために、 製品のシリアル番号を用意し、このお知らせのURLを知らせてください。 サポート契約をご利用でないお客様に対する無料アップグレードは、 TAC 経由でご要求いただく必要があります。 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、 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 PSIRTにおいて、現在本アドバイサリ内で記載されている脆弱性を悪用する事例や不正利用は確認されておりません。

この脆弱性はテクニカルサポート部門でのサービスリクエストの調査中に発見されました。

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 Cisco Systems 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

本アドバイザリーは、以下のシスコのワールドワイドウェブサイト上に掲載されます。

http://www.cisco.com/warp/public/707/cisco-sa-20090325-ctcp.shtml

ワールドワイドのウェブ以外にも、次の電子メールおよび Usenet ニュースの受信者向けに、この通知のテキスト版がシスコ PSIRT PGP キーによるクリア署名つきで投稿されています。

- 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
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

このアドバイザリに関する今後の更新は、いかなるものも Cisco のワールドワイドウェブに掲載される予定です。 しかしながら、前述のメーリングリストもしくは ニュースグループに 対し積極的に配信されるとは限りません。 この問題に関心があるお客様は上記 URL にて最新情報をご確認いただくことをお勧めいたします。

更新履歴

Revision 1.1	2009-June-25	Removed references to the March/09 combined fixed software table.
Revision 1.0	2009-March-25	Initial public release.

シスコセキュリティ手順

Cisco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支援、およびCiscoからセキュリティ情報を入手するための登録方法について詳しく知るには、Ciscoワールドワイドウェブサイトの http://www.cisco.com/en/US/products/products_security_vulnerability_policy.htm にアクセスしてください。このページにはCiscoのセキュリティ通知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。全てのCiscoセキュリティアドバイザリは http://www.cisco.com/go/psirt で確認することができます。