Cisco IOS cTCPのDoS脆弱性

アドバイザリーID : cisco-sa-20090325-ctcp CVE-2009-0635
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

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 Tunneling Control Protocol(cTCP)カプセル化機能を備えたEasy VPNサーバとして設定されたCisco IOSデバイスで、サービス拒否(DoS)状態が発生する可能性があります。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。回避策はありませんが、IPSec NATトラバーサル(NAT-T)機能を代替として使用できます。

このアドバイザリは、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ctcp で公開されています。

注： 2009年3月25日のCisco IOSセキュリティアドバイザリバンドル公開には8件のSecurity Advisoryが含まれています。これらのアドバイザリはすべて、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、そのアドバイザリに記載された脆弱性を修正するリリースが記載されています。

各ドキュメントへのリンクは次のとおりです。

- Cisco IOS cTCPのDoS脆弱性
  https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ctcp

- Cisco IOSソフトウェアの複数の機能におけるIPソケットの脆弱性
  https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ip

- Cisco IOSソフトウェアモバイルIPおよびモバイルIPv6の脆弱性

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-mobileip

- Cisco IOSソフトウェアのSecure Copyにおける権限昇格の脆弱性
  https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-scp

- Cisco IOSソフトウェアのSession Initiation ProtocolにおけるDoS脆弱性
  https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-sip

- Cisco IOSソフトウェアの複数の機能における巧妙に細工されたTCPシーケンスの脆弱性
  https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-tcp

- Cisco IOSソフトウェアの複数機能における巧妙に細工されたUDPパケットの脆弱性
  https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-udp

- Cisco IOSソフトウェアのWebVPNおよびSSLVPNの脆弱性
  https://sec.cloudapps.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以降を実行し、EZVPNサーバのCisco Tunneling Control Protocol(cTCP)カプセル化が設定されているCisco IOSデバイスには脆弱性が存在します。

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、デフォルトでは無効になっています。EZVPNクライアントが設定されているCisco IOSデバイスは、この脆弱性の影響を受けません。脆弱性が存在するのは、EZVPNサーバとして設定されているデバイスだけです。

Easy VPNにcTCPカプセル化機能を設定するには、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。オプションで、crypto ctcp port <port>コマンドを使用して、デバイスがリッスンするポート番号を指定できます。最大10個の番号を設定でき、ポート値は1 ~ 65535にすることができます。portキーワードが設定されていない場合、デフォルトのポート番号は10000です。次の例では、Cisco IOSデバイスがポート10000でcTCPメッセージをリッスンするように設定されています。

```
crypto ctcp port 10000
```

注：portキーワードが設定されているのは、EZVPNサーバとして動作するCisco IOSデバイスでだけです。

シスコ製品で稼働しているCisco IOSソフトウェアのバージョンを確認するには、デバイスにログインし、show versionコマンドを発行してシステムバナーを表示します。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。出力の次の行では、イメージ名がカッコで囲まれて表示され、その後に「Version」とIOSリリース名が続きます。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、シスコ製品でCisco IOSソフトウェアリリース12.3(26)が稼働し、インストールされているイメージ名が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の製品を示しています。

```
  Router#show version
  Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE SOFTWARE
  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リリースの命名規則の追加情報は、http://www.cisco.com/warp/public/620/1.htmlにある『White Paper: Cisco IOS Reference Guide』というドキュメントに記載されています。

脆弱性を含んでいないことが確認された製品

cTCPが設定されていない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シリーズコンセントレータには脆弱性はありません。EZVPNクライアントとして設定されているCisco IOSデバイスは、この脆弱性の影響を受けません。Cisco VPN Clientには脆弱性はありません。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、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 Tunneling Control Protocol(cTCP)機能は、標準IPSecが既存のファイアウォール規則を変更することなく透過的に機能しない環境で動作するEasy VPNリモートデバイスによって使用されます。cTCPトラフィックは、実際にはTCPトラフィックです。Cisco IOS cTCPパケットは、TCP経由で送信されるインターネットキーエクスチェンジ(IKE)パケットまたはEncapsulating Security Payload(ESP)パケットです。

一連のTCPパケットによって、cTCPカプセル化機能を備えたEasy VPNサーバとして設定されているCisco IOSデバイスのメモリが不足する可能性があるという脆弱性が存在します。この脆弱性は、Cisco Bug ID CSCsr16693（登録ユーザ専用）およびCSCsu21828(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-2009-0635が割り当てられています。

回避策

回避策はありません。

代わりに、IPSec NATトラバーサル(NAT-T)機能を使用することもできます。IPSec NAT-T機能は、NATとIPSecの間に数多く存在する既知の非互換性に対処することで、IP Security(IPSec)トラフィックがネットワーク内のネットワークアドレス変換(NAT)ポイントまたはポートアドレス変換(PAT)ポイントを通過することをサポートします。

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リリース12.2(13)T以降を実行しているルータでは、設定手順はありません。両方のVPNデバイスがNAT-Tに対応している場合、NATトラバーサルは自動的に検出され、ネゴシエートされます。

注：NAT-Tを有効にすると、Cisco IOSデバイスはすべてのIPSec対応インターフェイスでUDPポート4500を自動的に開きます。

注意： NAT-Tをサポートするには、Cisco VPNソフトウェアクライアントでIPSec over UDPを有効にする必要がある場合があることに注意してください。さらに、インターネットキーエクスチェンジ(IKE)用にUDPポート500、NAT-T用にUDPポート4500を許可するように、ファイアウォール規則を変更する必要がある場合があります。

NAT-Tの詳細については、次のURLにあるホワイトペーパーを参照してください。

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。

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20090325-ctcp

修正済みソフトウェア

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況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
影響を受ける 12.2 ベースのリリースはありません。		
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（2009年4月29日に入手可能）	12.4(22)T1 12.4(15)T9（2009年4月29日に入手可能）
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	

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco 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やその公表は確認しておりません。

この脆弱性は、テクニカルサポートサービスリクエストの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ctcp

改訂履歴

リビジョン 1.1	2009年6月25日	2009年3月9日の統合修正済みソフトウェアテーブルへの参照を削除。
リビジョン 1.0	2009年3月25日	初回公開リリース

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。