Cisco Security Advisory:TCP Vulnerabilities in Multiple Non-IOS Cisco Products

Revision 1.0

For Public Release 2004 April 20 21:00 UTC (GMT)

目次

要約

Transmission Control Protocol の仕様 (RFC793) に脆弱性があることが、 外部のある研究者によって発見されました。不正利用された場合は、かつて広く認知され ていたよりもはるかに短時間で任意の確立された TCP コネクションをリセッ トできます。ほとんどの場合、その切断の後にコネクションの再確立が短時 間のうちに行われる為、短時間のうちにリセットを繰り返し実行されない限 り、攻撃の影響に気づきません。

アプリケーションによっては、コネクション は自動的に再確立されます。その他の場合は、ユーザは再度操作 (Telnet や SSH セッションの新規オープン) を行う必要があります。攻撃を受けるプロ トコルによっては、攻撃の成功によるコネクションの切断後の考慮が必要な 派生的な影響があります。この攻撃は装置 (例、ルータ、スイッチ、コンピ ュータ) で終端するセッションのみが該当し、装置を通過するトラフィック (例、ルータによって転送されるトランジット (通過) トラフィック) は 影響を受けません。さらに、これによって直接的にデータの完全性や機密性が損なわれることはありません。

TCP プロトコルスタックを有する全てのシスコ製品は本脆弱性の影響を受けます。

本アドバイザリは Cisco IOS ソフトウェアが稼動する以外のシスコ製品の 脆弱性について記述したもので、以下にて確認可能です。

http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml

対となるアドバイザリは Cisco IOS ソフトウェアが稼動するのシスコ製品の 脆弱性についた記述

したもので、以下にて確認可能です。

http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml

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、英語原文が優先いたします。

該当製品

TCP プロトコルスタックを有する製品は本脆弱性の影響を受けます。 全てのシスコ製品、モデルが影響を受けます。本脆弱性による問題の深刻度は、 TCP を使用する上位プロトコルやアプリケーションに依存します。

この攻撃は装置（例、ルータ、スイッチ、コンピュータ）で終端するセッションのみ が該当し、装置を通過するトラフィック（例、ルータによって転送されるトランジット （通過）トラフィック）は影響を受けません。

完全に網羅しているわけではありませんが、影響を受ける non-IOS シスコ製品を 以下にリストします。

* Access Registrar

* BPX, IGX, MGX WAN switches, and the Service Expansion Shelf

* BR340, WGB340, AP340, AP350, BR350 Cisco/Aironet wireless products

* Cache Engine 505 and 570

* CallManager

* Catalyst 1200, 1900, 28xx, 29xx, 3000, 3900, 4000, 5000, 6000

* Cisco 8110 Broadband Network Termination Unit

* Cisco Element Management Framework

* Cisco Info Center

* Cisco Intelligent Contact Management

* Cisco MDS 9000

* Cisco ONS 15190/15194 IP Transport Concentrator

* Cisco ONS 15327 Metro Edge Optical Transport Platform

* Cisco ONS 15454 Optical Transport Platform

* Cisco ONS 15531/15532 T31 OMDS Metro WDM System

* Cisco ONS 15800/15801/15808 Dense Wave Division Multiplexing Platform

* Cisco ONS 15830 T30 Optical Amplification System

* Cisco ONS 15831/15832 T31 DWDM System

* Cisco ONS 15863 T31 Submarine WDM System

* Content Router 4430 and Content Delivery Manager 4630 and 4650

* Cisco Secure Intrusion Detection System (NetRanger) appliance and IDS Module

* Cisco Secure PIX firewall

* Cisco ws-x6608 and ws-x6624 IP Telephony Modules

* CiscoWorks Windows

* Content Engine 507, 560, 590, and 7320

* CSS11000 (Arrowpoint) Content Services Switch

* Hosting Solution Engine

* User Registration Tool VLAN Policy Server

* Cisco FastHub 300 and 400

* CR-4430-B

* Device Fault Manager

* Internet CDN Content Engine 590 and 7320, Content Distribution Manager 4670, and Content Router 4450

* IP Phone (all models including ATA and VG248)

* IP/TV

* LightStream 1010

* LightStream 100 ATM Switches

* LocalDirector

* ME1100 series

* MicroHub 1500,MicroSwitch 1538/1548

* Voice Manager

* RTM

* SN5400 series storage routers

* Switch Probe

* Unity Server

* VG248 Analog Phone Gateway

* Traffic Director

* WAN Manager

影響を受けないことが確認された製品

以下の製品に脆弱性はありません

* Cisco VPN 3000 Series Concentrators

* Cisco Firewall Services Module for Cisco Catalyst 6500 Series and Cisco 7600 Series (FWSM)

詳細

TCP はトランスポート層のプロトコルで、コネクション型で信頼性のある Internet Protocol (IP) パケットの配送を提供するように設計されています。 この実現のために、TCP は状態 (state) とパケットの再構築 (reassemble) するための順序を特定する順序番号 (sequence number) の混在するフラグを 使用します。また、TCP は応答番号 (acknowledgement number) と呼ばれる 期待する次のパケットの順序番号 (sequence number) を提供します。

パケットは"window" と呼ばれる、ある範囲の応答番号 (acknowledgement number) に順序番号 (sequence number) が入る場合にのみ、受信側の TCP スタック によって再構築されます。リセット (RST) フラグが設定される際は、さななる戻 りのパケットはないため、応答番号 (acknowledgement number) は使用されません。 TCP の完全な仕様は以下より入手可能です。

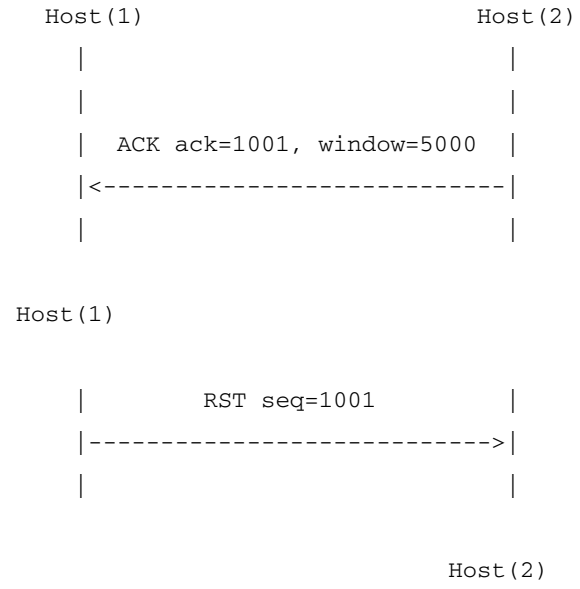
http://www.ietf.org/rfc/rfc0793.txt

RFC793 の仕様によると、確立された TCP コネクションは、reset (RST) もしくは synchronize (SYN) フラグをセットしたパケットを送信すること によってリセットすることが可能です。これ

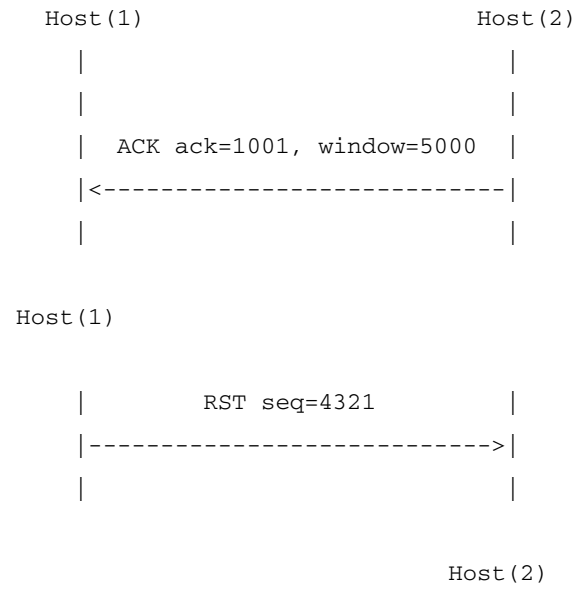
を実行するには 4-tuple (送信元、 宛先のIP と ポート) とともに順序番号 (sequence number) が既知あるいは 推測できることが前提となります。しかし、順序番号 (sequence number) は完全に一致する必要がなく、広告された window に収まっていれば十分で す。このことにより、敵対者が必要な労力は低減することとなります。

window が大きいほど、コネクションのリセットが容易となります。送信元、 宛先 IP アドレスが比較的容易に特定できるのに対して、送信元 TCP ポー トは推測しなくてはなりません。宛先 TCP ポートは通常、標準的なサービ ス (例、Telnet の 23、HTTP の 80) に関しては既知です。Cisco IOS は予 測可能な一時的なポート (番号) を予想可能な増分 (後続のコネクションに は次のポート (番号) が使用されます) で既知のサービスに使用します。こ れらの値は特定の IOS バージョンやプロトコルでは一定であってもリリー スによって異なります。

以下は通常の TCP セッションの終了の例です:



:



２つめの例で、順序番号 (sequence number) が次の期待するもの（すなわち 1001）でないにもかかわらず、どのように RST パケットがセッションを終了できたか 注目してください。広告された範囲の window に順序番号 (sequence number) が 収まっていれば十分なのです。この例では、Host(2) が順序番号 (sequence number) 1001 から 6001 を受信対象としています。そして 4321 はその範囲内にあります。

一般的には、TCP コネクションが 1 分以上確立されたままのプロトコルは影響が あると考えるべきです。セッションは再確立されるため、不正利用は多くの場合、 単に迷惑な行為にすぎません。

* Cisco IOS

Cisco IOS が稼動するすべての装置に脆弱性があります。 セッションのエンド・ポイントのみがこの脆弱性によって影響を受けるため、 装置そのもので終端するTCP セッションのみが影響を受けます。 装置を通過するセッションは、起点または終点の装置に脆弱性がある場合のみ 影響を受けますが、通過するルータそのものの上では攻撃不可能です。 本脆弱性によって、データの完全性や機密性は影響を受けません。影響を受ける のは可用性のみです。

本脆弱性は Cisco Bug Toolkit（登録のあるお客様のみ）で BugID CSCed27965 と CSCed38527 でドキュメントとして提供しております。

* Cisco IOS FireWall (IOS FW)

IOS FW はルータを通過するパケットを監視し、セッションの状態を内部的に 保持します。したがって、必要なポートを open し、トラフィックを通過させ セッション終了後にそれらを close することが可能です。IOS FW は 装置を通過するパケットすべてを傍受 (intercept) し調べるため、IOS FW を通過する TCP セッションはすべて攻撃の影響を受けることになります。 起点もしくは終点の装置に脆弱性がなくともこの事実はあてはまります。

本脆弱性は Cisco Bug Toolkit（登録のあるお客様のみ）で BugID CSCed93836 でドキュメントとして提供しております。

* Network Address Translation (NAT)

本脆弱性は NAT に関して一切影響はありません。NAT 機能は単純に ポート（番号）や IP アドレスを書き換えます。この機能は TCP フラグの解釈は 行わず、したがってこの攻撃に対して脆弱性はありません。しかし、攻撃 パケットはルータを通過し、受信する装置は影響されることがあります。

影響

影響は個別のプロトコルごとに異なります。ほとんどの場合において TCP コネクション は自動的に再確立される一方で、いくつかの特定のプロトコルではコネクション の切断による派生的な影響のほうがより大きい場合があります。Cisco PSIRT では TCP ベースの複数のプロトコルの解析を実施し、ご案内している利用方法の範囲に おいては、深刻な影響がないと確信しています。

長時間におよぶ潜在的により大きい 影響がある可能性のあるコネクションについて以下に解析の結果を示します。

Voice signaling H.225, H.245 (H.323 プロトコルスイートの一部)
H.225 と H.245 プロトコルは voice signaling に使用されます。それらは (voice あるいは video の) コンテンツ搬送のパラメーターを調整するため のものです。確立されたセッションは呼 (call) の間、維持されます。制御 (signaling) セッションが切断された場合は、呼 (call) も切断されます。 新たな制御 (signaling) セッションが、呼 (call) 設定時に新たに確立され ますが、切断された呼 (call) は再接続されることはありません。

IP Phone や Softphone は呼 (call) ごとに 1 つの制御 (signaling) セッション を生成します。制御 (signaling) セッションの切断は 1 ユーザーのみに影響があります。 1 つの制御 (signaling) セッションが複数の呼 (call) と関係していることがありますが、 そのセッションはサービスプロバイダーの内部ネットワークで使われるものです。 攻撃を実行するのに必要なパラメータをすべて特定するのはネットワークが現在の ベスト・プラクティスにのっとって設計されている場合は、容易な作業とはいえません。

Network Storage (iSCSI, FCIP)
ネットワーク・ストレージ製品は 2 種類の TCP ベースプロトコル、 SCSI over IP (iSCSI) と Fiber Channel over IP (FCIP) を使用します。

* SCSI over IP (iSCSI)

iSCSI はクライアント/サーバー環境において使用されます。クライアントは コンピューターで、クライアントのみがコネクションを設定します。 このコネクションは共有のものではありません。利用される仮想装置ごとに 別のセッションが確立されます。

現在のMicrosoft の Windows のドライバ・ソフトウェア、現在の Cisco の Linux のドライバ・ソフトウェアの利用者は、切断されたセッションによる派生的な 悪影響を受けません。これらのドライバ・ソフトウエアはセッションを再確立し 切断され時点から転送を再開します。他のベンダーのドライバ・ソフトウェアは 異なる挙動を示す可能性があります。

利用者は仮想装置 (virtual device) へのアクセスが通常より僅かに遅いと感じる 可能性があります。

* Fiber Channel over IP (FCIP)

FCIP は peer-to-peer のプロトコルです。スイッチ間のデータの複製に使用されます。 それぞれの peer はセッションを設定できます。スイッチは実際にはメッシュ状に 組まれます。 1 リンクがダウンした場合にはトラフィックは他のリンクへ迂回します。 敵対者がどうにかセッションを複数回連続して切断できた場合、ユーザー・アプリケーション は "Device unreachable" もしくは類似のエラーで終了する可能性があります。スイッチ そのものに影響はなく、利用者は再度操作を実施すればよいことになります。

利用者は仮想装置 (virtual device) へのアクセスが通常より僅かに遅いと感じる 可能性があります。

Transport Layer Security/Secure Socket Layer (TLS/SSL)
本脆弱性は TCP 層に関連する動作に存在するため、暗号化で保護できるもので はありません。SSL/TLS コネクションは様々なカプセル化でき、これらは は長時間コネクションになりえます。不正利用に成功した場合にも、データの 機密性には影響がありません。暗号化されたセッションは起点もしくは終点の ホスト、あるいは (もし設置されていれば) その前段にあるファイアーウォール で攻撃可能となります。

ソフトウェアバージョンおよび修正

Product	Defect ID	Intended First Fixed Release
LAN Switching		
Catalyst 1200, 1900, 28xx, 29xx, 3000, 3900, 4000, 5000, 6000	CSCed32349 (registered customers only)	No software availability date has been determined yet.
Catalyst 1900 and 2820	?/TD>	9.00.07 Available on 2004-Apr-27
Network Storage		
Cisco MDS 9000 Family	CSCed45453 (registered customers only)	1.3(3.8), 2.0(0.51)
Voice Products		
WS-6624 analog station gateway module for the Catalyst 6500	CSCee22691 (registered customers only)	No software availability date has been determined yet.
Wireless Products		
Cisco Aironet Access Point 340, 350, 1200 Series (only VxWorks-based)	CSCee22526 (registered customers only)	No software availability date has been determined yet. Customers are encouraged to migrate to IOS.
Security Products		
Cisco PIX Firewall	CSCed91445 (registered customers only)	6.3.3.132, 6.2.3.109, and 6.1.5.103 availability estimate: 2004-Apr-21
Optical Products		
Cisco ONS 15327,	CSCed73	4.62, 4.14, 2.25,

15454, 15454SDH and 15600 Optical Transport Platform	026 (registered customers only)	Available 2004-Apr-27

修正ソフトウェアの入手

契約を有するお客様

通常の経路でアップグレードのためのソフトウェアを入手してください。ほとんどのお客様は、シスコ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入手することができます。

http://www.cisco.com/tacpage/sw-center/

サードパーティによるサポートを受けているお客様

シスコパートナー、正規販売代理店等と、過去または現在の契約を通じてシスコ製品を購入、保守管理しているお客様は、その正規販売代理店を経由して無償ソフトウェアアップグレードを入手してください。

シスコサービス契約を結んでいないお客様

シスコから直接購入するもシスコサービス契約を結んでいないお客様、およびサード パーティーベンダーから購入し、そのベンダーから修正済ソフトウェアを入手できな いお客様は、次に示す連絡先を通じてシスコ Technical Assistance Center (TAC) に 連絡し、修正済ソフトウェアを入手して下さい。TAC への連絡先は以下の通りです。

+1 800 553 2447 (北米内からフリーダイヤル)

+1 408 526 7209 (北米以外からの有料通話)

e-mail: tac@cisco.com

様々な言語に対応する各地域専用の電話番号やダイヤル手順、電子メールアドレスな ど、その他の TAC 問い合わせ情報につきましては、こちらをご参照ください。

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

無償アップグレード資格がある証拠として、製品のシリアル番号と、この通知の URL を提示してください。契約がないお客様の無償アップグレードは TAC を通して要求し てください。

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。

回避策

回避策の効果は、お客様の状況、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によって異なります。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。

脆弱性の影響を緩和する利用可能な回避策はありません。

スプーフィング対策をネットワーク境界に適用することにより、 脆弱性にさらされる危険性を低減することが可能です。

uRPF を有効にすれば、すべてのスプーフパケットは、機能が有効になっている最初の 装置で破棄されます。uRPF を有効にするには以下のコマンドを使用します。

router(config)#ip cef
router(config)#ip verify unicast reverse-path

uRPF がどのように動作し、様々な状況に応じてどのように設定するかにつきま しては、以下をご参照ください。

http://cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7d4.html

ftp://ftp-eng.cisco.com/cons/isp/security/URPF-ISP.pdf

これは、特に非対称ルーティング (asymetric routing) を使用している場合は 特に重要です。

ACL は境界になるべく近くで設定されるべきです。uRPF と異なり許可する IP の 明確な範囲を指定する必要があります。遮断されるべき IP アドレスを特定する のは、維持するのが困難になりがちで最適な解決策ではありません。

注意：スプーフィング対策を有効にするには、保護する装置の最低 1 ホップ先の 装置に設定される必要があります。理想的にはネットワーク境界において 設定します。

不正利用事例と公表

Cisco PSIRT では本アドバイザリに記載されている脆弱性を利用した不正利用事例は確認 していません。

RST フラグ(リセットパケット) を利用した本脆弱性の不正利用は、OSVDB.org の Paul (Tony) Watson によって発見されました。それを SYN フラグの利用に拡張 した攻撃方法については、解決に協力するベンダーによって発見されました。

この通知のステータス：INTERIM

この内容は INTERIM 通知です。シスコ PSIRT では本通知の内容すべてに関して 完全性を保証いたしかねますが、すべて公表事実は最善を尽くして確認されているものに なります。シスコ PSIRT では通知における事実に変更がない限り新たなバージョンを リリースする予定はなく、重

要な変更がある場合にのみ本通知を更新します。

後述する情報配信の URL を省略し、本アドバイザリーの記述内容に関して、独自の複製・ 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-20040420-tcp-nonios.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
* bugtraq@securityfocus.com
* first-teams@first.org (includes CERT/CC)
* cisco@spot.colorado.edu
* comp.dcom.sys.cisco
* firewalls@lists.gnac.com

この通知に関する今後の最新情報は、いかなるものもシスコ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 1.0	2004-April-20	初版

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支援、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につい て詳しく知るには、シスコワールドワイドウェブサイトの

http://www.cisco.com/warp/public/707/sec_incident_response.shtml

にアクセスしてください。 このページにはシスコ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。
全てのシスコ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。