Cisco Security Advisory: Crafted ICMP Messages Can Cause Denial of Service

Revision 1.2

最終更新日 2005 年 4 月 22 日 22:30 (GMT)

公開日 2005 年 4 月 12 日 12:00 (GMT)

目次

要約

インターネット コントロール メッセージ プロトコル (ICMP) を利用したトランスミッション コントロール プロトコル (TCP) への

サービス妨害攻撃 (Denial of Service (DoS) attack) が可能なことが記述されているドキュメントがあり、そのドキュメントは、インターネット エンジニアリング タスクフォース(IETF)のドラフト "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt)として公開されています。

これらの攻撃は、その機器自体がセッションを終端しているか、発信している時のみ影響があり、

1. ICMP "hard error"メッセージを使用した攻撃、
2. パス最大伝送ユニット(PMTU)への攻撃として知られる、ICMP "Fragmentation needed and Don't Fragment (DF) bit set"メッセージを使用した攻撃、
3. ICMP "source quench"メッセージを使用した攻撃、

の3種類があります。攻撃のタイプにより既存コネクションのリセットか通信速度の低下を引き起こす可能性があります。

このインターネットドラフトに記述された攻撃により、シスコの複数の製品が影響を受けます。

シスコでは、本脆弱性対処用の無償のソフトウェアを提供しています。 また、場合によっては本脆弱性の影響を緩和する回避策 もあります。

本アドバイザリは以下にて確認可能です。
http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml

本脆弱性の公開については、英国の National Infrastructure Security Coordination Centre (NISCC)が調整を行っています。NISCCは、影響を受ける可能性のある製品を製造する会社とともに作業を行っており、その情報は以下にて確認可能です

http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en

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。

該当製品

脆弱性が存在する製品

Cisco IOS

IOSが動作するシスコ製品で、デフォルト設定もしくは明示的に設定されてPMTUDが動作する場合、影響を受けます。すべてのバージョンのIOSで影響があります。脅威の深刻度は、プロトコルやアプリケーションがどれだけ特定のPMTUDメッセージに依存するかによります。IOSは、ICMP "hard error" や、"souce quench"メッセージを 使用した攻撃に対しては脆弱ではありません。

Cisco 製品で稼動中のソフトウェアを確認するには、機器にログインし **show version**コマンドを実行し、システムバナーを画面に表示します。 Cisco IOS ソフトウェアは "Internetwork Operating System Software" もしくは単に "IOS" と表示します。そのすぐ後ろにイメージ名が括弧の間に 表示され(場合により改行されています)、続いて "Version" と IOS リリース名が表示されます。 (IOS 以外の)他の Cisco の機器は " **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。

以下の例は Cisco 製品で IOS リリース 12.2(15)T14、イメージ名 C806-K9OSY6-M が稼動していることを示しています:

```
gw>show version
Cisco Internetwork Operating System Software
IOS (tm) C806 Software (C806-K9OSY6-M), Version 12.2(15)T14, RELEASE SOFTWARE (fc4)
[...]
```

以下のプロトコルはPMTUDを利用し、ネットワーク内の IOS 機器にこれらが設定された場合、PMTUDへの攻撃に対して脆弱になります。

- **TCP over IPv4**：BGP でのピアのように、IOS 機器が他の機器と TCP セッシ ョンを確立している場合で、PMTUD が設定されていると、細工された ICMP "Fragmentation needed and Don't Fragment (DF) bit set" エラ ーメッセージに対して脆弱です。
-
-
- **TCP over IPv6**：PMTUD は IPv6 でのデフォルト設定であり、IPv6が設定さ れている機器で、もし BGP のように TCP を利用するサービスが有効な場合、 PMTU D攻撃に対して脆弱で

す。機器が単に IPv6 トラフィックを転送す るだけで、他の端末と TCP セッションを確立しない場合、影響は受けま せん。

-
-
- **IP Security (IPSec)**: IOS機器は、IPsecが設定されると PMTUD がデフォ ルトで動作するため、本ドキュメントで示すPMTUD攻撃に影響を受ける ようになります。IOS機器で**crypto map** か **tunnel protection** が インターフェースで設定されるような IPsec 設定のときです。

設定の例:

```
crypto ipsec profile IPSEC_PROFILE
 [...]
!
crypto map MYMAP 1 ipsec-isakmp
 [...]
!
interface Tunnel0
 tunnel protection ipsec profile IPSEC_PROFILE
 [...]
!
interface Ethernet1
 crypto map MYMAP
 [...]
```

- **Generic Routing Encapsulation および IPinIP**：これらのトンネルの設定 がされた機器で PMTUD が有効な場合、細工された ICMP "fragmentation needed and DF bit set" メッセージに対して脆弱です。これらの 2 つのプロト コルの PMTUD デフォルト設定は停止です。 設定で **tunnel path-mtu-discovery**が記述されている機器が脆弱とな ります。
-
-
- **Layer 2 Tunneling Protocol(L2TP) Version 2 と、Layer 2 Tunneling Protocol Version 3(L2TPv3)**：これらのトンネルの設定がされた機器で PMTUD が有効な場合、細工された ICMP "fragmentation needed and DF bit set"メッセージに脆弱です。これらの2つのプロトコルのPMTUDデ フォルト設定は停止です。L2TPが動作する機器で、**ip pmtu** 設定がさ れている場合に脆弱となります。

  注： L2TP (version 2) と L2TPv3 (version 3)は、2つのそれぞれ別の 独立したプロトコルですが、両方とも影響を受け、また同じような影響 のされ方をするので、このドキュメントでは１つとして扱います。

IOSベースのルータに加え、以下の製品は Cisco IOS か、IOS を元にしたソフトウェアが動作するため、脆弱性が存在します：

- Catalyst 4000、6000 スイッチ がI OS をハイブリッド(Supervisor Engine で CatOS、Multilayer Switch Feature Card で IOS が動作)か、ネイテ ィブ(Supervisor Engineで IOS が動作)モードで動作する場合。
- Cisco Aironet Wireless LAN アクセスポイントと、ブリッジ
- Catalyst 2900XL、2900XL-LRE、3500XL、2940、2950、2950-LRE、2955 および 2970 シリーズスイッチ

- Catalyst 2948G-L3、3550、3560、3750、and 3750-ME シリーズスイッチ
- Communication Media Module (CMM)
- Cisco Optical Network Solutions (ONS) products: ONS 15454 と ONS 15530/15540で利用される ML と SL blades
- Cisco Distributed Director

IOS 以外の製品

以下の IOS 以外の製品も同様に脆弱性が存在します：

- Cisco CRS-1：CRS-1のIOS XR においても、CRS-1 が BGP のような TCP を使 用したアプリケーションで他の機器とセッションを確立する場合、PMTU D 攻撃や ICMP "hard error" メッセージを使用した攻撃に脆弱性が存在 します。 IOS XR の PMTUD のデフォルト設定は停止ですが、機器で tcp path-mtu-dis covery が設定された場合に PMTUD が動作となります。 show version コマ ンドを使用することで IOS XRのバージョン情報を得ることができます。
- Cisco Secure PIX Security Appliance: PIX で IPSec が設定されている場合、PMTUD 攻撃に対する脆弱性が存在します。影響を受けるトラフィックは攻撃を受けた特定の IPSec トンネルのみです。
  PIX firmware の デフォルトでは IPSec は停止です。
  PIX で IPSec が動作するのは、機器のインターフェースに crypto map 設定がある場合で、コマンドは以下になります。

  crypto map <crypto map name> interface <interface name>

  show versionコマンドにより、PIX で動作しているバージョン情報を得 ることができます。
  PIX Security Appliance ソフトウエアのバージョン 7.0 以降はこれらの脆弱性の影響を受けません 。
-
-
- Cisco IP Phones
  - 7940/7960 with Skinny Client Control Protocol (SCCP) firmware.
  - 940/7960 with Session Initiation Protocol (SIP) firmware.
  - 7970 with Skinny Client Control Protocol firmware (細工され た ICMP "hard error" メッセージに対してのみ脆弱)

  Cisco IP Phone で動作しているファームウェアは、電話の "Settings" を押し、"Status" メニュオプションを選ぶことで得ることができます。
- Cisco Catalyst 6608 Voice Gateway と Cisco 6000 FXS Analog Inter face Module (WS-X6624-FXS)： 細工された ICMP "hard error" メッセージと、ICMP "source quench" メッ セージに対して脆弱です。 6608 と 6624 ファームウェアのバージョンは Catalyst 6500シリーズ スイッチにログインし show version コマンドを実行することで得ら れます。
- Global Site Selector (GSS).
-
-
- Cisco ONS products: ONS 15302 and ONS 15305.
-
-
- Cisco MDS 9000 Series Multilayer Switches.
-
-

- VPN 5000 concentrator.
-
-
- Cisco MGX-8250 (PXM-1 based) および MGX-8850 (PXM-1E and PXM-45 based) - コントロールプレインのみ脆弱です、スイッチングサービスには影響がありません。
-
-
- Cisco Content Switching Module (CSM) - コントロールプレインのみ脆弱です、スイッチングサービスには影響がありません。

脆弱性が存在しない製品

以下の製品では本脆弱性の影響を受けません：

- Cisco Firewall Services Module (FWSM) for Cisco Catalyst 6500 Series and Cisco 7600 Series.
- Cisco Guard and Cisco Traffic Anomaly Detector Denial of Service mitigation appliances.
- Catalyst Switches.
  以下の Catalystスイッチで IOS が動作していない場合、本ドキュメン トで記述された脆弱性の影響を受けません：
  - 1200
  - 1700
  - 1900
  - 2100
  - 28xx
  - 2948G-GE-TX
  - 2900, 2902, 2926T and 2926G
  - 3000, 3100, 3200
  - 3900
  - 5000
  - Catalyst 4000、6000 スイッチでは CatOS か IOS を動作させること ができます。CatOS で動作する場合、Multilayer Switch Feature Card (MSFC) が無ければ、脆弱性はありません(MSFC は IOS で動作す るため)。IOS 動作する場合、上記の[脆弱性が存在する製品」で書かれたように、脆弱性が存在します。
- Cisco ONS products:
  - ONS 15327 Metro Edge Optical Transport Platform
  - ONS 15454 Optical Transport Platform(MSPP and MSTP)
  - ONS 15531/15532 T31 OMDS Metro WDM System
  - ONS 15216 EDFA3/EDFA2/OADM
  - ONS 15310 CL.
- Cisco IP Phones
  - ATA 186/188
  - 7910
  - 7912
  - 7902/5
  - 7920
- Cisco VG248 Analog Phone Gateway
- Cisco MeetingPlace.

- シスコ VPN 3000 Series Concentrators, VPN 3002 Hardware Clients, VPN Software Client (注意：VPN Software Client 自体に脆弱性は存在し ませんが、VPN clients が動作している OS は影響を受けるはずです。 利用している OS の製造者にご確認ください)
- Cisco BTS 10200 Softswitch
- Cisco Application and Content Networking System (ACNS) ソフトウェアが稼動する。 Content Engine、Content Router および Content Distribution Manager。
- Cisco Local Director

Microsoft Security Bulletin MS05-019によると Microsoft Windows は PMTUD 攻撃および ICMP "hard error" メッセージによる攻撃に対して脆弱性が存在します。 以下の voice and IP communication 製品は Microsoft Windows OSと共に出荷され、また、その上で動作します。 しかし、 これらの製品に同梱されている現行の Microsoft Windows (release 2000.2.5)はシスコで作成され、PMTUD はデフォルトで停止です。 (release 200.2.4 およびそれ以前は Microsoft のデフォルトの通り PMTUD が動作します) これらの製品が脆弱性が存在するのは、 利用者が明示的に PMTUD を動作させ、かつ Microsoft WindowsがこのICMP脆弱性に影響を受ける場合となります。

- Cisco Call Manager.
- Cisco IP Interactive Voice Response.
- Cisco IP Call Center Express.
- Cisco IP Queue Manager.
- Cisco Personal Assistant.
- Cisco Emergency Responder.
- Cisco Conference Connection.
- Cisco Internet Service Node.

以下の製品はシスコでカスタマイズした Microsoft Windows を使用していません。Microsoft Security Bulleting MS05-019の記述の通り
Microsoft Windows では PMTUD はデフォルトで動作することとなるため、 これらの製品で設定の変更をしていない場合は PMTUD 攻撃に対する脆弱性が存在するはずです。また、ICMP "hard error" メッセージに対しても脆弱性が存在します。

- Cisco Unity.
- Cisco IP Contact Center Enterprise Edition.

シスコ製品と共に使用しているMicrosoft WindowsでPMTUDが動作しているかどうかは、下記のレジストリキーを確認してください。:

```
HKEY_LOCAL_MACHINE¥System¥CurrentControlSet¥Services¥Tcpip¥Parameters¥EnablePMTUDisco
very
```

レジストリーキーが存在する場合、PMTUD はキーの値によって動作･停止が決定されます。キーが存在しない場合、PMTUD は動作します。

Cisco Secure ACS Solution Engine (Cisco Secure ACS Appliance) は Microsoft Windows をベースとしており、従って PMTUD 攻撃および ICMP "hard error" メッセージ による攻撃に対する脆弱性が存在します。しかし、最近の ACS Solution Engine は Cisco Security Agent (CSA) とともに出荷されており、それはICMP メッセージを一切 受信しないように設定されています。この状態において Cisco Secure ACS Solution Engine は本ドキュメントに記載された脆弱性は存在しません。

ICMP echo request (ping) を ACS Appliance に送信してみることで CSA がインストールされてい

て動作しているか確認できます。（返送された）ICMP echo reply が受信された場合は CSA が 動作していないかインストールされていないことになります。

CSA が利用可能か確認するためには "System Configuration:Upgrade Appliance" でどのバージョンがインストールされているか確認し、"System Configuration: Appliance Configuration" で CSA が 動作しているか確認します。

該当製品略記

以下の表はシスコ製品が本脆弱性に影響を受けるかどうかを略記したものです。

製品	Hard エラー	PMTUD	Source Quench
IOS	影響なし	影響あり	影響なし
IOS XR	影響あり	影響あり	影響なし
IP Phones	影響あり	影響あり	影響あり
PIX Security Appliance	影響なし	影響あり	影響なし
Catalyst 6608 and 6624	影響あり	影響なし	影響あり
Cisco 11000 and 11500	影響なし	影響なし	影響あり
Cisco GSS	影響なし	影響なし	影響あり
MDS 9000	影響なし	影響あり	影響あり
Cisco VPN 5000 Concentrator	影響なし	影響あり	影響なし
Some ONS products	影響なし	影響あり	影響なし
Cisco MGX-8250 and MGX-8850	影響あり	影響あり	影響あり
Cisco Content Switching Module	影響なし	影響なし	影響あり
Voice and IP Communication Products Using Cisco-Customized Microsoft Windows	影響あり	影響あり	影響なし
Cisco ACS Solution Engine	影響あり	影響あり	影響なし

1つの製品にいくつかのモデルがある場合、それぞれで異なる影響を受けることがあます。 追加の情報については 詳細の項を御参照ください。

詳細

ICMP は TCP/IP プロトコルの重要な要素で、エラー情報や診断情報を提供します。 ICMP エラーメッセージはセッションのエンドシステムあるいは中継ルータのいずれにおいても生成される可能性があります。 エンドシステムや中継ルータは受け取った ICMP エラーメッセージで報告されたエラーのタイプにより異なった動作をとります。 ICMP で報告されるエラーには "hard error" と "soft error" の二種類があります。

RFC 1122 ("Requirements for Internet Hosts - Communications Layers" - http://www.ietf.org/rfc/rfc1122.txt)は、 3 つの "hard error"（"protocol unreachable", "port unreachable" and "fragmentation needed and Don't Fragment bit set"）と 5 つの "soft error"（"network unreachable", "host unreachable", "source route failed", "time exceeded", and "parameter problem"）を 定義しています。これ以外のICMPエラーメッセージとして、"source quench" がホストにより生成されることがあります。 "source quench" が "hard error" なのか "soft error" なのか RFC1122 には明確な記述がありませんが、 それを受け取ったホストの振る舞いを考えると "soft error" と考えるべきです。なぜなら、この時ホストは ICMP "source quench"

メッセージを 生成したホストへの送信データレートを暫くの間減少させ、その後次第に送信レートを増加させるからです。

ICMP エラーメッセージの "Fragmentation needed and Don't Fragment bit set" (type 3, code 4)は RFC 1191 ("Path MTU discovery" - http://www.ietf.org/rfc/rfc1191.txt) の PMTU Discovery と呼ばれる重要なメカニズムに使用されます。 このメカニズムにより TCP/IP プロトコルは Path MTU を動的に決めることが出来るため、 IP パケットの分割を最小限に防ぎ帯域を有効利用することが出来ます。このメカニズムはホストにとり必須のものではありませんが、 それを実装したホストは "Fragmentation needed and Don't Fragment bit set" メッセージを受け取ると "soft error" として 処理しなければなりません。IPパケットの分割とPMTUDが分割を防ぐ仕組みに関しては、シスコのホワイトペーパー "IP Fragmentation and PMTUD" (http://www.cisco.com/en/US/tech/tk827/tk369/technologies_white_paper09186a00800d6979.shtml . をご参照ください。

ICMP により報告される "hard error" と "soft error" の違いにより、それを受け取ったホストの動作は異なります。 一般的には、TCPのようなコネクション型のプロトコルにおいてICMP "hard error" を受け取った場合にはそのコネクションを開放します。 またICMP "soft error" を受け取ったホストはそのエラーを引き起こした状況を解消しようとします。

インターネットドラフト"ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt)には、ICMPを用いてTCPプロトコルに対するDOS攻撃を行なう方法について記述されています。 これらの攻撃を行なうには通信を行なう両ホストの IP アドレス (と TCP の場合) ポート番号を知る必要がありますが、 コネクションをリセットしたりスループットを低下させることが出来ます。

注：これらの攻撃はそのデバイスが始点・終点となるセッションにのみ影響し、中継トラフィック、 すなわちそのデバイスを通過し他のデバイスで終端するトラフィックには影響がありません。

細工された ICMP "hard error"メッセージによる攻撃

ICMP "hard error" メッセージを受け取ったホストは、エラーメッセージの示す相手のホストとのコネクションを開放しなければなりません。 このホストは必ずしもICMPメッセージを生成したシステムである必要はなく、IP ヘッダーと ICMP ペイロードに埋め込まれた トランスポート・プロトコルデータにより一意に識別されます。コネクションを開放する理由は、"hard error" が復旧困難な深刻な ネットワークの問題を意味するからです。細工された ICMP "hard error" メッセージのために、ホストは実際には問題のないコネクションを 開放してしまうかもしれません。 この種の攻撃をインターネットドラフト "draft-gont-tcpm-icmp-attacks-03.txt" では "blind connection-reset" に分類しています。

PMTUDに対する攻撃

ホスト上で PMTUD が動作していた場合、細工された"fragmentation needed and DF bit set" ICMPメッセージにより Path MTU を 非常に小さな非現実的な値に設定することが出来ます。この時スループットが非常に低下するため、 コネクションが確立しているにも関わらず上位レイヤのプロトコルにおいてタイムアウトが発生する可能性があります。 この種の攻撃をインターネットドラフト "draft-gont-tcpm-icmp-attacks-03.txt" では "throughput-reduction"に分類しています。

RFC1191 の PMTUD アルゴリズムによると、その実装において学習した MTU は時間の経過とともに更新されなければなりません。 つまりMTUは時間の経過とともに最適値に戻りますが、それには最大１０分程度かかります (RFC 1191は１０分を推奨していますが要求事項ではなく、 従ってその値は実装に依存します) 。しかしながら、もし細工された "Fragmentation needed and DF bit set" ICMP メッセージが 脆弱性を持つホストに継続的に送り続けられたなら、DoS 状態に陥るために学習した MTU が更新されることはありません。

前述の通り、もしホスト上で PMTUD が動作していなければ ICMP "Fragmentation needed and DF bit set" メッセージは "hard error" と見なされます。このため PMTUD 攻撃によりコネクションのリセットを引き起こす可能性もあります。

TCP のように分割のリスクを最小限にするためにトランスポート層の MTU と Maximum Segment Size (MSS)を 用いるプロトコルにおいては、コネクションが攻撃を受けているかどうかを判定する良い方法は このトランスポート層の MTU が非現実的なくらい小さな値に設定されているかどうかをモニターすることです。 シスコIOSにおいてこの手法を用いる例を本ドキュメントに後述します。

注：TCPを利用する多くのプロトコルは PMTUD 攻撃の影響を受ける可能性があります。 その例としては、BGP、Hyper Text Transfer Protocol (World Wide Web で使用されるHTTP)、 the Simple Mail Transfer Protocol (電子メイルで使用されるSMTP)、そして SSH (Secure Shell)があります。 Data-Link Switching (DLSw)、Serial Tunneling (STUN)、そして Block Serial Tunneling (BSTUN) といった IBM プロトコルセットにはトランスポートプロトコルにTCPを利用するように設定ができるものもあります。 Domain Name System (DNS)は通常 UDP を使いますが、ゾーン転送などでは UDP の代わりに TCP を使用します。

細工された "source quench" ICMP メッセージによる攻撃

前述のように、ICMP "source quench" メッセージを受け取ったホストはそれを生成したホストへの送信データレートを減少させます。 TCP/IPの実装や使用するトランスポート層プロトコルにより ICMP "source quench" メッセージに対するレスポンスは変わりますが、 一般的には ICMP "source quench" メッセージを受け取ったホストは輻輳回避アルゴリズムを起動するべきです。

TCPを使用するホストが ICMP "source quench" メッセージを受信した場合、 再送信タイムアウトが起きたかのようにスロースタートを起動することをRFC 1122は推奨しています。 RFC 2001 ("TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms" - http://www.ietf.org/rfc/rfc2001.txt)は近年のTCPの実装に用いられるスロースタートと輻輳回避アルゴリズムについて記述しており、実際にはスロースタートと輻輳回避アルゴリズムは共に実装されていると述べています。

より低レートでデータを送信すると、ICMP "source quench" メッセージを生成したホストは受信バッファが空きになるまで処理します。

"source quench" メッセージを更に受け取らなければ時間の経過とともにウィンドウ・サイズは合理的な値に戻りますが、 細工された "source quench" メッセージにより通信効率が劇的に低下する可能性があります。 もし攻撃者が繰り返し細工した "source quench" メッセージを送り続けたならコネクション上のサービスの低下が続くことになります。

この種の攻撃はインターネットドラフト "draft-gont-tcpm-icmp-attacks-03.txt" では "throughput-reduction" に分類しています。

シスコ製品への影響

本ドキュメントに記述されたICMPによる攻撃の影響はシスコ製品により異なります。製品によっては特別なコンフィグレーションやネットワーク・プロトコルを設定した時に影響を受けます。ここではシスコ製品がどのようにこの脆弱性の影響をうけるのか、及びその条件について記述します。また各製品の関連するBug IDについても述べます。

Cisco IOS

シスコIOSには ICMP "hard error" メッセージによる攻撃に対する脆弱性は存在しません。何故なら IOS はコネクションが "established" 状態かどうかのチェックを行い、"non-established"状態の

時にのみ "hard error" メッセージに対する処理を行なうからです。

更に、シスコIOSは ICMP "source quench" メッセージを受け取っても処理しませんので、 細工された "source quench" メッセージによる攻撃に対する脆弱性も存在しません。

該当製品セクションで述べたように、IOS には PMTUD 攻撃に対する脆弱性が存在します。 すなわちICMP "Fragmentation needed and DF bit set" メッセージ（IPv6の場合には"packet too big" メッセージ）を細工することにより、 Path MTUを変えることが出来ます。以下に IOS の各プロトコルにおいて PMTUD の脆弱性に関連する Bug ID を示します。

- **PMTUD を用いる全プロトコル**: CSCef60659 （登録ユーザのみ） -- ICMP unreachableに対するより厳重なチェックが必要である。
- **TCP over IPv4**: CSCed78149 （登録ユーザのみ） -- IPv4 上で PMTUD を起動する TCP コネクションは細工された ICMP に対して脆弱である。

  コネクションが PMTUD 攻撃を受けているかどうかを判定する良い方法は、コネクションの MSS 値をチェックすることです。 次の例にあるように、BGP セッションに対しては、**show ip bgp neighbors | include Data** コマンドにより 最大データセグメント長を意味する MSS 値を表示します。

```
Router#show ip bgp neighbors | include data segment
Datagrams (max data segment is 1460 bytes):
Router#
```

  理論上 MTU サイズの最小値は 68 バイトですが、今日のインターネットにおいては 576 バイト以下の MSS 値は疑わしいと考えるべきです。 RFC1191の7章にはインターネットで共通に用いられるMTUサイズがリストされています。 他の TCP コネクションに対しては、**show tcp brief** コマンドによってそのコネクションの TCB を特定し、 その TCB を用いた **show tcp tcb <tcb identified with show tcp brief>| include data segment** コマンドにより MSS 値を表示することが出来ます。

```
Router#show tcp brief
TCB        Local Address           Foreign Address        (state)
00E97148   192.168.100.1.23        192.168.100.1.11002    TIMEWAIT
00E97A78   192.168.100.1.23        192.168.100.1.11003    ESTAB
00E975E0   192.168.100.1.11003     192.168.100.1.23       ESTAB
Router#show tcp tcb 0x00E975E0 | include data segment
Datagrams (max data segment is 1474 bytes):
Router#
```

  この手法はTCP over IPv6においても適用可能です。
- **TCP over IPv6**: CSCef61610 （登録ユーザのみ） -- ICMPv6メッセージの処理の過ちのためTCPのパフォーマンスが低下する。
- **IP Security**: CSCsa59600 （登録ユーザのみ） --IOS IPSecコネクションは細工されたICMPパケットに対して脆弱であり、そのため特定フローのPMTUが非常に小さな値になることがある。 RFC1191によると、細工されたICMP "fragmentation needed and DF bit set"メッセージによりPMTUサイズが小さくなった後更にICMP "fragmentation needed and DF bit set"メッセージを受け取らなければ、一旦学習したMTUサイズは10分間有効でありその後PMTUは first-hopのデータリンクMTUサイズに戻されます。.

IPSec トンネルが PMTUD 攻撃を受けているかどうかを調べるには、以下の例のように **show crypto ipsec sa | include mtu** コマンドを用いる方法があります。

```
Router#show crypto ipsec sa | include mtu
  path mtu 1500, media mtu 1500
Router#
```

- **Generic Routing Encapsulation及び IPinIP**: CSCef44699 （登録ユーザのみ） --GRE と IPIP トンネルは細工された ICMP パケットに対して脆弱です。GREとIPIPトンネルがPMTUD攻撃を受けているかどうかを調べるには、以下の例のように **show interface tunnel <number> | include Path MTU** コマンドを用いる方法があります。

  Router# show interface tunnel 0 | include Path MTU Path MTU
  Discovery, ager 10 mins, MTU 1476, expires never

- CSCef44699
- 登録ユーザのみ
- **tunnel path-mtu-discovery min-mtu<minimum MTU>**
-

  %TUN-5-IGNOREICMPMTU Tunnel1 ignoring received ICMP Type 3 Code 4,
  due to pmtud min-mtu setting

- **Layer 2 Tunneling Protocol Version 2 とLayer 2 Tunneling Protocol Version 3**: L2TPv3に対しては、CSCsa52807 （登録ユーザのみ） -- PMTUD を起動する L2TPv2 は細工された ICMP パケットに対して脆弱です。L2TPv3に対しては、CSCef43691（登録ユーザのみ） -- PMTUD を起動する L2TPv3 は細工された ICMP パケットに対して脆弱です。L2TPv2セッションがPMTUD攻撃を受けているかどうかを調べるには、以下の例のように **show vpdn session all | include Session MTU** コマンドを用いる方法があります。

  Router#**show l2tun session all | include Session MTU**
  Session PMTU enabled, path MTU is 32 bytes
  Session PMTU enabled, path MTU is 32 bytes
  Session PMTU enabled, path MTU is 32 byte

- CSCsa52807
- 登録ユーザのみ
- **vpdn pmtu minimum <minimum MTU>**
- **vpdn pmtu maximum <maximum MTU>**
- **vpdn-group**
  %VPDN-5-IGNOREICMPMTU Ignoring received ICMP Type 3 Code 4,
  due to pmtu min or max setting

IOS XR

IOS XR には ICMP "hard error" メッセージによる攻撃と PMTUD への攻撃に対する脆弱性があります。 この脆弱性に関する Bug ID はCSCef45332（登録ユーザのみ） --CRS-1 コネクションは

細工された ICMP パケットに対して脆弱です。IO-XRは ICMP "source quench" メッセージを処理しませんのでこのタイプの攻撃に対する脆弱性は存在しません。

Cisco IP Phones

いくつかのモデルの Cisco IP Phone には、ICMP "hard error" メッセージや ICMP "source quench" メッセージによる攻撃、 PMTUDへの攻撃に対する脆弱性が存在します。

- CSCef46728（登録ユーザのみ） -- SCCP ファームウェアが動作する 7940/7960 IP Phone は細工された ICMP "hard error" メッセージに対して脆弱です。
- CSCef54947（登録ユーザのみ） -- SCCP ファームウェアが動作する 7970 IP Phone は細工された ICMP "hard error" メッセージに対して脆弱です
- CSCef54204（登録ユーザのみ） -- SIP ファームウェアが動作する 7940/7960 IP Phone は細工された ICMP "source quench" メッセージに対して脆弱です。 ただし SIP で動作する 7940/7960 IP Phone はシグナリング用に TCP を使用ないため、この脆弱性が該当するのは IP Phone への telnet セッションと IP Phone から（例えばディレクトリサーバーへ）の HTTP セッションに限られます。
- CSCef54206（登録ユーザのみ） -- SIPファームウェアが動作する 7940/7960 IP Phone は細工された ICMP "hard error" メッセージに対して脆弱です。 ただしSIPで動作する 7940/7960 IP Phone はシグナリング用に TCP を使用しないため、この脆弱性が該当するのは IP Phone への telnet セッションと IP Phone から（例えばディレクトリサーバーへ）の HTTP セッションに限られます。

Cisco Secure PIX Security Appliance

RFC1191とRFC2401("Security Architecture for the Internet Protocol" - http://www.ietf.org/rfc/rfc2401.txt)に基づき、 IPSec を設定した PIX Security Appliance は積極的に PMTUD を行ないます。つまり ICMP "Fragmentation needed and DF bit set" メッセージを受信した際、 PIX Security Appliance は特定の IPSec フロー上の Path MTU を動的に学習・調整します。

従って PIX Security Appliance は Path MTU を非常に小さな値に設定しようとする細工された ICMP Type 3、Code 4 メッセージに対して脆弱です。 この脆弱性はBug ID CSCef57566（登録ユーザのみ） -- IPSecを設定したPIX Security Applianceは、パスやSAに対して非常に小さなPMTUを提示する 細工された ICMP パケットに対して脆弱である -- に記述されています。この現象は IPSec にて PMTUD が動作している場合に発生しますが、 PIX の場合にはIPSecを設定すると PMTUD は自動的にイネーブルになります。

Catalyst 6608 and 6624

Digital PRY Gateway、Conference Bridge、Transcoder/MTP firmware が動作する Cisco Catalyst 6000 Voice E1/T1 and Services Module (WS-X6608-E1 および WS-X6608-T1) 、Cisco Catalyst 6000 FXS Analog Interface Module (WS-X6624-FXS) は ICMP "hard error" および "source quench" メッセージによる攻撃に対する脆弱性が存在します。
これらの脆弱性は Cisco Bug ID CSCsa60692（登録ユーザのみ) -- ICMP Hard error handling. にドキュメントされています。

Cisco 11000、11500 Content Services Switches

マネージメントポートにおいて、シスコ11000、11500 Content Service Switchは ICMP "source quench" メッセージによる攻撃に対して脆弱性が存在します。 CSS は PMTUD を実行しません

ので PMTUD 攻撃に対しては脆弱ではありません。 ICMP "source quench" メッセージの脆弱性は BugID CSCeh45454（登録ユーザのみ） -- ICMP エラーパケットによるTCPへの攻撃 -- に記述されています。

Cisco Global Site Selector

バージョン 1.2 およびそれ以前の Cisco Global Site Selector には ICMP "source quench" メッセージに対する脆弱性が存在します。
Global Site Selector は ICMP "hard error" メッセージによる攻撃と PMTUD 攻撃に対して脆弱ではありません。
ICMP "source quench" メッセージの脆弱性は BugID CSCeh20083（登録ユーザのみ) -- ICMP エラーパケットによる TCP への攻撃 -- に記述されています。

Cisco MDS9000 シリーズ Multilayer Switches

Cisco MDS9000 シリーズ Multilayer Switch には PMTUD攻撃に対して脆弱性が存在します。 この脆弱性はBug ID CSCeh04183（登録ユーザのみ）-- TCPに対するICMPの攻撃 -- に記述されています。

Cisco ONS Products

Cisco ONS 製品は PMTUD 攻撃に関してのみ脆弱性があります。

VPN 5000 Concentrator

VPN 5000 ConcentratorはPMTUD攻撃に関して脆弱性があります。ICMP "source quench" メッセージはメッセージカウントを保持するために処理しますが輻輳回避の処理は行わないため、 VPN 5000 ConcentratorはICMP "source quench" メッセージによる攻撃に対して脆弱性はありません。 PMTUD 攻撃の脆弱性はBug ID CSCeh59823（登録ユーザのみ)-- ICMP 3/4メッセージは IPSec セッションに影響する -- に記述されています。

影響

細工されたICMP "hard error" メッセージによる攻撃のためにコネクションが切断されることがあります。

"Fragmentation needed and DF bit set" メッセージ(あるいは PMTUD攻撃)および ICMP "source quench" エラーメッセージのために コネクションのスループットが非常に低下する事があります。スループットが低下した場合にはホストの送信バッファのオーバーフローやパケットロスが発生したり、 あるいは必要以上にフラグメンテーションが起こりアプリケーションの通信効率に影響することがあります。 従って、細工された ICMP パケットにより Border Gateway Protocol（BGP)、Label Distribution Protocol (LDP) や Data-Link Switching (DLSw) といった ネットワークプロトコルに影響をおよぼす可能性があります。

スループットの低下に加え、PMTUD 攻撃を受けるとフラグメント化されたパケットの再構成のために余計に時間とメモリを消費するため、 CPU 使用率やメモリ消費量が増大する可能性があります。

これらのケースでは攻撃を受けた結果 DoS 状態となりますが、この攻撃のためにリモートによるコードの実行や認可されないアクセスを引き起こすことはありません。

ソフトウェアバージョンおよび修正

ソフトウェアアップグレードをご検討される際には、以下も併せてご参照ください。 http://www.cisco.com/en/US/products/products_security_advisories_listing.html また、後続のアドバイザリもご参照ください。

製品がアップグレードに必要なメモリを実装しているか、 現行のハードウェアとソフトウェアの構成が新リリースでもサポートされているか を十分ご確認ください。ご不明な点がありましたら、Cisco Technical Assistance Center (TAC) までご連絡ください。 IOS XR ソフトウエアをご利用いただいているお客様で修正ソフトウェアが必要な場合は Cisco TAC までご連絡ください。

IOS 製品

以下の Cisco IOS ソフトウェアの表の各行は、対象となるリリーストレイン、プラットフォームおよび 製品群を示します。あるリリーストレインが脆弱である場合、修正が組み込まれている最も早いリリース（最初に修正されたリリース）とそれが利用可能となる予定日が "Rebuild" and "Maintenance" の列に 示されます。リリーストレインで示されたリリースより前のものを使用している機器は脆弱であることが知られています。 使用するリリースは少なくとも示されたリリース以降へアップグレードすることが推奨されます。

"Rebuild" および "Maintenance" の用語に関する情報は以下をご参照ください。

http://www.cisco.com/warp/public/620/1.html

ソフトウェアが利用可能になる予定が異なることや、Cisco IOS が脆弱であるフィーチャーの条件が 異なるために、最初に修正されたリリースの表は脆弱性の影響を受ける各テクノロジーごとに分割されています。 以下の 4 つのグループがあります。

1. **TCPv4**: CSCed78149 （登録ユーザのみ）は TCP の PMTUD 攻撃に対する脆弱性に関して管理する Cisco Bug ID です。
2. トンネル:CSCef60659 （登録ユーザのみ）, CSCef43691 （登録ユーザのみ）, CSCsa61864 （登録ユーザのみ）, CSCsa59600 （登録ユーザのみ）, and CSCef44699 （登録ユーザのみ）. は影響を受けるトンネリングプロトコル の多く（GRE、L2TPv3 および IPSec) の脆弱性を管理する Cisco Bug ID です。
3. **TCPv6**: CSCef61610 （登録ユーザのみ）,は IPv6 上で稼動する TCP の PMTUD 攻撃に対する脆弱性を管理する Cisco Bug ID です。
4. **L2TPv2**: CSCsa52807 （登録ユーザのみ）, は L2TPv2 の PMTUD 攻撃に対する脆弱性を管理する Cisco Bug ID です。

Major Release		Availability of Repaired Releases	
Affected 12.0-Based Release		Rebuild	Maintenance
12.0	TCPv4 and Tunnels	12.0(28c)	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.0DA	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(12)DA8 or later	
	TCPv6	Not vulnerable	

	L2TPv2	Not vulnerable	
12.0DB	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.0DC	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(15)BC2f or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.0S	TCPv4 and Tunnels	12.0(27)S5, available 23-May-05	12.0(31)S, available 28-Apr-05
		12.0(28)S3, available 25-Apr-05	
		12.0(30)S1	
	TCPv6	12.0(27)S5, available 23-May-05	12.0(31)S, available 28-Apr-05
		12.0(28)S3, available 25-Apr-05	
		12.0(30)S1	
	L2TPv2	Not vulnerable	
12.0SC	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(15)BC2f or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.0SL	TCPv4 and Tunnels	Vulnerable; migrate to 12.0S or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.0SP	TCPv4 and Tunnels	Vulnerable; migrate to 12.0S or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.0ST	TCPv4 and Tunnels	Vulnerable; migrate to 12.0S or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	

12.0SX	TCPv4 and Tunnels	Vulnerable; contact TAC
	TCPv6	Vulnerable; contact TAC
	L2TPv2	Not vulnerable
12.0SZ	TCPv4 and Tunnels	Vulnerable; migrate to 12.0S or later
	TCPv6	Vulnerable; migrate to 12.0S or later
	L2TPv2	Not vulnerable
12.0T	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(27) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0W5	TCPv4 and Tunnels	12.0(25)W5(27c) 12.0(28)W5(31a)
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0WC	TCPv4 and Tunnels	12.0(5)WC12, available 25-July-05
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XA	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(27) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XB	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(27) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XC	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(27) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XD	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(27) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable

12.0XE	TCPv4 and Tunnels	Vulnerable; migrate to 12.1E latest
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XF	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(27) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XG	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(27) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XH	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(27) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XI	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(27) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XJ	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(27) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XK	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(28) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XL	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(28) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XM	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(27) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XN	TCPv4	Vulnerable; migrate to 12.1(27) or

	and Tunnels	later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XQ	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(27) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XR	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(28) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XS	TCPv4 and Tunnels	Vulnerable; migrate to 12.1E latest
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.0XV	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(27) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
Affected 12.1-Based Release	**Rebuild**	**Maintenance**
12.1	TCPv4 and Tunnels	12.1(27)
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1AA	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(28) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1AX	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(25)EY or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1AZ	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(22)EA4 or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable

12.1DA	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(12)DA8 or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1DB	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1DC	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(15)BC2f or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1E	TCPv4 and Tunnels	12.1(22)E6, available 02-May-05 12.1(23)E3, available 02-May-05 12.1(26)E1
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1EA	TCPv4 and Tunnels	12.1(22)EA4
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1EB	TCPv4 and Tunnels	Vulnerable; contact TAC
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1EC	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(15)BC2f or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1EO	TCPv4 and Tunnels	12.1(19)EO4, available 26-May-05
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1EU	TCPv4 and	Vulnerable; migrate to 12.2(20)EU or later

	Tunnels	
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1EV	TCPv4 and Tunnels	Vulnerable; contact TAC
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1EW	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(18)EW3 or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1EX	TCPv4 and Tunnels	Vulnerable; migrate to 12.1E latest
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1EY	TCPv4 and Tunnels	Vulnerable; migrate to 12.1E latest
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1T	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(28) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XA	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(28) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XB	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(28) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XC	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(28) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XD	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(28) or later

	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XE	TCPv4 and Tunnels	Vulnerable; migrate to 12.1E latest
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XF	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(28) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XG	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XH	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(28) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XI	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(28) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XJ	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XL	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XM	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XP	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable

	L2TPv2	Not vulnerable
12.1XQ	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XR	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XT	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XU	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1XV	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1YA	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1YB	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1YC	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.1YD	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable

12.1YE	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.1YF	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.1YH	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.1YI	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.1YJ	TCPv4 and Tunnels	Vulnerable; migrate to 12.1(22)EA4 or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
Affected 12.2-Based Release		**Rebuild**	**Maintenance**
12.2	TCPv4 and Tunnels		12.2(28)
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.2B	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.2BC	TCPv4 and Tunnels	12.2(15)BC2f	
	TCPv6	Not vulnerable	
	L2TPv2	Vulnerable; contact TAC	
12.2BW	TCPv4 and	Vulnerable; migrate to 12.3(13) or later	

	Tunnels		
	TCPv6	Not vulnerable	
	L2TPv2	Vulnerable; migrate to 12.3 or later	
12.2BY	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Not vulnerable	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.2BZ	TCPv4	Vulnerable; migrate to 12.3(7)XI3	
	Tunnels	Vulnerable; migrate to 12.3(7)XI5, available TBD	
	TCPv6	Not vulnerable	
	L2TPv2	Vulnerable; contact TAC	
12.2CX	TCPv4 and Tunnels	12.2(15)BC2f	
	TCPv6	Not vulnerable	
	L2TPv2	Vulnerable; contact TAC	
12.2CY	TCPv4 and Tunnels	12.2(15)BC2f	
	TCPv6	Not vulnerable	
	L2TPv2	Vulnerable; contact TAC	
12.2CZ	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Not vulnerable	
	L2TPv2	Vulnerable; contact TAC	
12.2DA	TCPv4 and Tunnels	12.2(12)DA8	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.2DD	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.2DX	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.2EU	TCPv4 and		12.2(20)EU

	Tunnels		
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Not vulnerable	
12.2EW	TCPv4 and Tunnels	12.2(18)EW3	
	TCPv6	Vulnerable; migrate to 12.2S	
	L2TPv2	Not vulnerable	
12.2EWA	TCPv4 and Tunnels	12.2(25)EWA	
	TCPv6	12.2(25)EWA	
	L2TPv2	Not vulnerable	
12.2EX	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(25)SEB or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.2EY	TCPv4 and Tunnels	12.2(25)EY	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.2JA	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(4)JA	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.2JK	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Vulnerable; contact TAC	
12.2MB	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Vulnerable; contact TAC	
12.2MC	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T	
	TCPv6	Vulnerable; migrate to 12.3(14)T	
	L2TPv2	Vulnerable; migrate to 12.3(14)T	
12.2S	TCPv4 and Tunnels	12.2(14)S13 12.2(18)S8	

		12.2(20)S7	
		12.2(25)S3	
	TCPv6	12.2(20)S7	
		12.2(25)S3	
	L2TPv2	Not vulnerable	
12.2SE	TCPv4 and Tunnels	12.2(25)SEB	
	TCPv6	12.2(25)SEA vulnerable; migrate to 12.2(25)SEB	
	L2TPv2	Not vulnerable	
12.2SO	TCPv4 and Tunnels	12.2(18)SO1, available 25-Mar-05	
	TCPv6	12.2(18)SO2, available 29-Apr-05	
	L2TPv2	Not vulnerable	
12.2SU	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Not vulnerable	
12.2SV	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(25)S3	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.2SW	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.2SX	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(17d)SXB7	
	TCPv6	Vulnerable; migrate to 12.2(17d)SXB7	
	L2TPv2	Not vulnerable	
12.2SXA	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(17d)SXB7	
	TCPv6	Vulnerable; migrate to 12.2(17d)SXB7	
	L2TPv2	Not vulnerable	
12.2SXB	TCPv4 and Tunnels	12.2(17d)SXB7	

	TCPv6	12.2(17d)SXB7	
	L2TPv2	Not vulnerable	
12.2SXD	TCPv4 and Tunnels	12.2(18)SXD4	
	TCPv6	12.2(18)SXD4	
	L2TPv2	Not vulnerable	
12.2SY	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(17d)SXB7	
	TCPv6	Vulnerable; migrate to 12.2(17d)SXB7	
	L2TPv2	Not vulnerable	
12.2SZ	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(20)S7	
	TCPv6	Vulnerable; migrate to 12.2(20)S7	
	L2TPv2	Not vulnerable	
12.2T	TCPv4 and Tunnels	12.2(15)T15	
	TCPv6	12.2(15)T15	
	L2TPv2	Vulnerable; contact TAC	
12.2XA	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.2XB	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later	
	TCPv6	Not vulnerable	
	L2TPv2	Vulnerable; migrate to 12.3 or later	
12.2XC	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Not vulnerable	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.2XD	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later	
	TCPv6	Not vulnerable	
	L2TPv2	Vulnerable; migrate to 12.3 or later	
12.2XE	TCPv4 and	Vulnerable; migrate to 12.3(13) or later	

	Tunnels	
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2XF	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(15)BC2f
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; contact TAC
12.2XG	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2XH	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2XI	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2XJ	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2XK	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2XL	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2XM	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2XN	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later

	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2XQ	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2XR	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(4)JA
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.2XT	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2XU	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2XW	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2YA	TCPv4 and Tunnels	12.2(4)YA9
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; contact TAC
12.2YB	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2YC	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2YD	TCPv4	Vulnerable; migrate to 12.3(14)T or

	and Tunnels	later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2YE	TCPv4 and Tunnels	Vulnerable; migrate to 12.2S or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.2S or later
12.2YF	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2YG	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2YH	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2YJ	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2YK	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.2YL	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later
12.2YM	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3(14)T or

		later
12.2YN	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later
12.2YO	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(17d)SXB7
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.2YQ	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later
12.2YR	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later
12.2YT	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Vulnerable; migrate to 12.3(12) or later
	L2TPv2	Vulnerable; migrate to 12.3 or later
12.2YU	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Vulnerable; migrate to 12.3(14)T or later
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later
12.2YV	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Vulnerable; migrate to 12.3(14)T or later
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later
12.2YW	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later

	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later
12.2YX	TCPv4 and Tunnels	Vulnerable; contact TAC
	TCPv6	Not vulnerable
	L2TPv2	Not vulnerable
12.2YY	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later
12.2YZ	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(20)S7
	TCPv6	Vulnerable; migrate to 12.2(20)S7
	L2TPv2	Not vulnerable
12.2ZA	TCPv4 and Tunnels	Vulnerable; migrate to 12.2(17d)SXB7
	TCPv6	Vulnerable; migrate to 12.2(17d)SXB7
	L2TPv2	Not vulnerable
12.2ZB	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Not vulnerable
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later
12.2ZC	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later
	TCPv6	Vulnerable; migrate to 12.3(14)T or later
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later
12.2ZD	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T
	TCPv6	Vulnerable; migrate to 12.3(14)T
	L2TPv2	Vulnerable; migrate to 12.3(14)T
12.2ZE	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(13) or later
	TCPv6	Vulnerable; migrate to 12.3(12) or

		later	
	L2TPv2	Vulnerable; migrate to 12.3 or later	
12.2ZF	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.2ZG	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.2ZH	TCPv4 and Tunnels	12.2(13)ZH6, available TBD	
	TCPv6	12.2(13)ZH6, available TBD	
	L2TPv2	12.2(13)ZH6, available TBD	
12.2ZJ	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.2ZK	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.2ZL	TCPv4 and Tunnels	12.2(15)ZL2, available TBD	
	TCPv6	12.2(15)ZL2, available TBD	
	L2TPv2	12.2(15)ZL2, available TBD	
12.2ZN	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or	

		later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.2ZP	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Vulnerable; contact TAC	
Major Release		**Availability of Repaired Releases**	
Affected 12.3-Based Release		**Rebuild**	**Maintenance**
12.3	TCPv4 and Tunnels	12.3(3h); available 21-Apr-05	12.3(13)
		12.3(5e); available 28-Apr-05	
		12.3(6e)	
		12.3(9d); available 21-Apr-05	
		12.3(10c)	
		12.3(12b); available 12-Apr-05	
	TCPv6	12.3(6e)	12.3(12)
		12.3(3h); available 21-Apr-05	
		12.3(5e); available 28-Apr-05	
		12.3(9d); available 21-Apr-05	
		12.3(10c)	
	L2TPv2	12.3(6e)	12.3(15), available 6-Jun-05
		12.3(3h); available 21-Apr-05	
		12.3(5e); available 28-Apr-05	
		12.3(9d); available 21-Apr-05	
		12.3(12b);	

		available 12-Apr-05	
		12.3(13a); available 2-May-05	
12.3B	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.3BC	TCPv4 and Tunnels	12.3(9a)BC2	
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Vulnerable; contact TAC	
12.3BW	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(7)T8 or later	
	TCPv6	Vulnerable; migrate to 12.3(7)T8 or later	
	L2TPv2	Vulnerable; migrate to 12.3(11)T4 or later	
12.3JA	TCPv4 and Tunnels		12.3(4)JA
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.3T	TCPv4 and Tunnels	12.3(7)T8	12.3(14)T
		12.3(8)T7	
		12.3(11)T4	
	TCPv6	12.3(7)T8	12.3(14)T
		12.3(8)T7	
		12.3(11)T4	
	L2TPv2	12.3(11)T4	12.3(14)T
		12.3(7)T10; available 16-May-05	
12.3XA	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.3XB	TCPv4	Vulnerable; migrate to 12.3(14)T or	

	and Tunnels	later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.3XC	TCPv4 and Tunnels	12.3(2)XC3, available TBD	
	TCPv6	12.3(2)XC3, available TBD	
	L2TPv2	12.3(2)XC3, available TBD	
12.3XD	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.3XE	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.3XF	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.3XG	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Vulnerable; contact TAC	
12.3XH	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	

12.3XI	TCPv4	12.3(7)XI3	
	Tunnels	12.3(7)XI5, available TBD	
	TCPv6	12.3(7)XI3	
	L2TPv2	Vulnerable; contact TAC	
12.3XJ	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Vulnerable; contact TAC	
12.3XK	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.3XL	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.3XM	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.3XQ	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.3XR	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.3XS	TCPv4 and	Vulnerable; migrate to 12.3(14)T	

	Tunnels		
	TCPv6	Vulnerable; migrate to 12.3(14)T	
	L2TPv2	Vulnerable; migrate to 12.3(14)T	
12.3XT	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(4)JA	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.3XU	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Vulnerable; contact TAC	
12.3XW	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(11)YF2 or later	
	TCPv6	Vulnerable; migrate to 12.3(11)YF2 or later	
	L2TPv2	Vulnerable; migrate to 12.3(11)YF2 or later	
12.3XX	TCPv4 and Tunnels	Vulnerable; migrate to 12.3(14)T or later	
	TCPv6	Vulnerable; migrate to 12.3(14)T or later	
	L2TPv2	Vulnerable; migrate to 12.3(14)T or later	
12.3XY	TCPv4 and Tunnels	12.3(8)XY4	
	TCPv6	Not vulnerable	
	L2TPv2	Not vulnerable	
12.3YA	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Vulnerable; contact TAC	
12.3YD	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Vulnerable; contact TAC	
12.3YF	TCPv4 and Tunnels	12.3(11)YF2, available 12-May-05	
	TCPv6	12.3(11)YF2, available 12-May-	

		05	
	L2TPv2	12.3(11)YF2, available 12-May-05	
12.3YG	TCPv4 and Tunnels	12.3(8)YG1	
	TCPv6	12.3(8)YG1	
	L2TPv2	Vulnerable; contact TAC	
12.3YH	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Vulnerable; contact TAC	
12.3YI	TCPv4 and Tunnels		12.3(8)YI
	TCPv6		12.3(8)YI
	L2TPv2		12.3(8)YI
12.3YJ	TCPv4 and Tunnels	Vulnerable; contact TAC	
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Vulnerable; contact TAC	
12.3YK	TCPv4 and Tunnels		12.3(11)YK
	TCPv6		12.3(11)YK
	L2TPv2	Vulnerable; contact TAC	
12.3YN	TCPv4 and Tunnels		12.3(11)YN
	TCPv6	Vulnerable; contact TAC	
	L2TPv2	Vulnerable; contact TAC	
12.3YQ	TCPv4 and Tunnels		12.3(14)YQ
	TCPv6		12.3(14)YQ
	L2TPv2		12.3(14)YQ

IOS 以外の製･

IOS 以外の製品

以下の IOS 以外のソフトウェアの表の各行は、対象となるリリーストレイン、プラットフォームおよび 製品群を示します。あるリリーストレインが脆弱である場合、修正が組み込まれている最も早いリリース（最初に修正されたリリース）とそれが利用可能となる予定日が "Rebuild" and

"Maintenance" の列に 示されます。リリーストレインで示されたリリースより前のものを使用している機器は脆弱であることが知られています。 使用するリリースは少なくとも示されたリリース以降へアップグレードすることが推奨されます。

Product	Bug ID	First Fixed Release
IOS XR	CSCef45332（登録ユーザのみ）	SMU ID AA01157 for IOS XR 3.0.0 Download from https://www.cisco.com/cgi-bin/Support/FileExg/IOSXR_30.cgi SMU ID AA01172 for IOS XR 3.0.1 Download from https://www.cisco.com/cgi-bin/Support/FileExg/IOSXR_30.cgi
7960 (SCCP)	CSCef46728（登録ユーザのみ）	7.1(1)
7970 (SCCP)	CSCef54947（登録ユーザのみ）	6.0(3)
7960 (SIP)	CSCef54204（登録ユーザのみ） and CSCef54206（登録ユーザのみ）	Release date not determined yet.
Cisco PIX Security Appliance	CSCef57566（登録ユーザのみ）	6.2.4(101) and 6.3.4(120), both available from http://www.cisco.com/pcgi-bin/tablebuild.pl/PIXPSIRT.
Catalyst 6608 and 6624	CSCsa60692（登録ユーザのみ）	D00404000018 (load 18, DSP Ver 4.3.25) for the 6608 and A00204000010 (load 10, DSP Ver 4.3.25) for the 6624.
Cisco 11000 and 11500 Content Services Switches	CSCeh45454（登録ユーザのみ）	Release date not determined yet.
Cisco Global Site Selector	CSCeh20083（登録ユーザのみ）	Release date not determined yet.
Cisco MDS 9000 Series Multilayer Switches	CSCeh04183（登録ユーザのみ）	SAN-OS 2.1(1a)
VPN 5000 Concentrator	CSCeh59823	Please contact TAC.
ONS 15454 IOS-based blades (ML and SL)	See Cisco bug IDs for Cisco IOS	R5.0
ONS 15302 and ONS 15305	-	R2.0
Cisco MGX-8250 and MGX-8850	CSCeh65337（登録ユーザのみ） and CSCeh63449（登録ユ	Release date not determined yet

	ーザのみ ） for the Cisco MGX2	
Voice and IP Communication Products Using Cisco-Customized Microsoft Windows	-	win-OS-Upgrade-k9.2000-2-7sr3.exe; available 26-Apr-2005
Cisco ACS Solution Engine	CSCeh62307 （ 登録ユーザのみ ）	Release date not determined yet

他社製のオペレーティングシステム(OS)が稼動するすべてのシスコ製品で、シスコから OS が提供されないものに関しては 関連するベンダーから適切なパッチを入手してください。

修正ソフトウェアの入手

ご契約を有するお客様

ご契約を有するお客様は、修正ソフトウェアが利用可能になり次第、通常の経路でそれを 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/.

シスコパートナー、正規販売代理店等とのご契約を有するお客様

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機器を購 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。

ご契約のないお客様

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ください。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。ご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。

回避策の実装に際して支援が必要な場合、または、回避策に関するご質問がある場合は テクニカルアシスタンスセンター(TAC) までご連絡ください。

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/warp/public/687/Directory/DirTAC.shtml を参照してください。

お客様におかれましては、ご購入いただきましたフィーチャーセットに関してのみ インストール

いただくことができ、サポートさせていただきます。インストール、 ダウンロード、アクセス、その他ソフトウェアアップグレードされた場合は、 以下の Cisco Software License Term に従うことに同意したものとします。 http://www.cisco.com/public/sw-license-agreement.html http://www.cisco.com/public/sw-center/sw-usingswc.shtml.

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。

PMTUD を停止する影響

後述の通り、細工された ICMP "fragmentation needed and DF bit set" メッセージ (ICMPv6 の場合 "message too big" メッセージ) による攻撃による影響を緩和する最も一般的な回避策は 可能な範囲で PMTUD を設定により停止することです。

PMTUD を停止することによる悪影響は通常の場合はないことに留意することが重要になります。 PMTUD を停止した場合、機器は DF bit を設定せずにデータグラムを送信します。大きなパケットが MTU が小さいルータに到達した場合、ルータはパケットをより小さなものに分割します。より小さい 分割されたデータは宛先に到達し元の大きなパケットが再構築されます。

PMTUD が停止されると特に TCP が影響を受けるのは、TCP は Path MTU の変動を反映せず、Maximum Segement Size(MSS) を調整しないためです。そのため実際に使用される MSS の値が Path MTU の値よりも大きい場合には不要なセグメンテーションが発生します。 使用される MSS の値は設定コマンドにより手動で設定された値が、設定されない場合はデフォルトの値として 宛先が local 以外の場合は 536 バイト、local の場合は MSS - 40 バイト (IP ヘッダサイズ 20 バイト分と TCP ヘッダ 20 バイト分合算) が使用されます。
不要なセグメンテーションの発生を回避するためには MSS をデータパスの最小 MTU を通過できるように小さく設定することをお勧めします。

注) Cisco IOS を使用する際、実装により PMTUD が停止されている場合は MSS 値を手動 (コマンド **ip tcp mss <MSS value>**) で設定できません。PMTUD が停止されている場合、 宛先が local 以外の場合は 536 バイト、local の場合はインターフェイス MTU - 40 バイト (例 Ethernet の場合 1460 バイト) が使用されます。

最後に、通常 PMTUD を停止しても既存の接続には影響がなく、既存の接続は手動で終了し再接続する 必要がある点にご留意ください。

Voice アプリケーション、PIX Security Appliance と PMTUD

Voice アプリケーションが稼動する機器 (例 Cisco CallManager) で PMTUD を停止した場合、Cisco Secure PIX Security Appliance をトラフィックが通過しており PIX が SCCP (**fixup protocol skinny**)、 SIP (**fixup protocol sip**) や H.323 (**fixup protocol h323**) などの Voice プロトコル の Fixup を行っている場合、期待しない状況を引き起こす場合があります。

注) デフォルトでは Cisco CallManager は PMTUD が停止されています

PIX Security Appliance/FWSM ソフトウェアは、分割された Voice 制御トラフィックのプロトコルデータユニット(PDU)を 完全にはインスペクション出来ない場合があるため問題が発生する可能性があります。 PMTUD を停止している場合、大きな PDU が複数の TCP セグメントや IP フラグメントに 分割されると、多くの場合に、メディアトラフィックが通過する穴を適切に開けることが できなくなる状況が発生し得ます。

従って、Voice アプリケーションが稼動する機器で PMTUD を停止する場合、必要な後続のメディアトラフィック を許可し、関連するプロトコルの Fixup を停止するアクセス制御ルールの用意を考慮する必要があります。

事前にポートをオープンしておく必要があることにより、利用者のセキュリティポリシーによっては、 PMTUD を停止する回避策が利用できない場合があります。

ICMP Unreachable メッセージを遮断する際の影響

特に IPSec や他の PMTUD を停止できない製品の場合は、回避策として、 ICMP "fragmentation needed and DF bit set" メッセージを遮断する方法があります。 重要なのはこのメッセージを遮断するのは、保護する機器宛のメッセージであり、ネットワーク内の 他の機器宛のメッセージではないことを承知しておくことです。無差別にこのメッセージを遮断した 場合、RFC 2923 "TCP Problems with Path MTU Discovery" -http://www.ietf.org/rfc/rfc2923.txt に記述されている「ブラックホール」を形成する可能性があることを予め承知しておくことです。

さらに、ICMP "fragmentation needed and DF bit set" メッセージがエンドホストが受信できないように 遮断されている場合、エンドホストは DF bit をクリアにして送信しなくてはなりません。これは PMTUD を停止したり、他に方法がない場合はサポートされている環境においては "crypto ipsec df-bit clear" などの特別な手法を用いて実現できます（IPSec の場合）。

ICMP unreachable が遮断されていて、パケットに DF bit がセットされて送信される場合は PMTU に対してパケットが大きすぎて中継ルータでパケットの分割が必要な場合（送信元（エンドホスト）で パケットを分割か、DF bit をクリアにして再送信が必要な場合）にも、エンドホストは 適切な対応をとることができません。

Cisco IOS の回避策

IP version 4(IPv4) 上の Transmission Control Protocol(TCP)

PMTUD が明示的に設定されている場合、PMTUD に対する攻撃を防止するには グローバル設定コマンド "**no ip tcp path-mtu-discovery**" を用いて PMTUD を停止する回避策があります。コマンドが実行されると新たな TCP 接続における PMTUD は停止されます。IOS 機器では PMTUD の設定変更によりその機器を 始点もしくは終点とする既存の TCP セッションへの影響はありません。

PMTUD が停止されている場合、 MSS は "**ip tcp mss**" コマンドにより設定された値か デフォルトの値として、宛先が local 以外の場合は 536 バイト、 local の場合は MSS - 40 バイト（IP ヘッダサイズ 20 バイト分と TCP ヘッダ 20 バイト分合算）が使用されます。

IP version 6(IPv6) 上の Transmission Control Protocol(TCP)

IPv6 上で TCP を使用する場合はデフォルトで PMTUD が設定されており、停止することができません。 そのため、Access Control List(ACL) により ICMPv6 "packet too big" メッセージを遮断する回避策を お勧めします。

ICMPv6 "packet too big" メッセージを遮断することはレイヤ 3 (IPv6) PMTUD も停止する することであり、エンドホストでの MTU を IPv6 MTU の最低値である 1280 バイトに設定しなくてはならない 点にご留意ください。機器は "packet too big" メッセージを確認できず、中継システムでパケットが 大きすぎるために廃棄されていることを検知できないためです。

ICMPv6 "packet too big" メッセージは IPv6 において ICMPv4 "fragmentation needed and DF bit set" に相当するメッセージです。したがって、ICMPv6 "packet too big" メッセージを遮断するに

あたっては 「ICMP Unreachable メッセージを遮断する際の影響」は同様に該当します。

IPSec

IPSec につきましては PMTUD を停止する回避策をお勧めします。 IPSec の場合は単一コマンドで PMTUD を停止できないものの他の方法で実現できる点をご留意ください。 具体的には、以下の 2 つを実施していただく必要があります。

1. Access Control List(ACL) または Control Plane Policing (CoPP) を用いてルータ宛の ICMP "fragmentation needed and DF bit set" メッセージ (Type 3, Code 4) を遮断します。

   以下の例でどのように機器のインターフェイスから入る ICMP Type 3, Code 4 メッセージを遮断するか示します。 (Type 3, Code 4 メッセージは packet-too-big キーワードで指定しています)

```
access-list 111 deny icmp any host <fa0/0's IP address> packet-too-big
access-list 111 deny icmp any host <fa0/1's IP address> packet-too-big
access-list 111 deny icmp any host <fa0/2's IP address> packet-too-big
access-list 111 permit ip any any
!
interface fastEthernet 0/0
  ip access-group 111 in
!
interface fastEthernet 0/1
  ip access-group 111 in
!
interface fastEthernet 0/2
  ip access-group 111 in
```

   注) この回避策が効果的なのは、ACL にすべてのルータの IP アドレスを含め、且つ、 ACL をすべてのインターフェースに適用した場合です

   この方式はベストプラクティスの 1 つであるインフラストラクチャー ACL(iACLs)の構成要素として 設定できます。iACLs に関するさらなる情報は以下をご参照ください。
   "Protecting Your Core: Infrastructure Protection Access Control Lists"
   http://www.cisco.com/warp/public/707/iacl.html

   .

   以下の例ではどのように Control Plane Policing で同様に実現するか示します。

```
access-list 140 permit icmp any host <interface0 IP address> packet-too-big
access-list 140 permit icmp any host <interface1 IP address> packet-too-big
[...]
access-list 140 permit icmp any host <interfaceN IP address> packet-too-big
access-list 140 deny   ip   any any
!
class-map match-all icmp-class
  match access-group 140
!
policy-map control-plane-policy
```

```
  ! Drop all traffic that matches the class "icmp-class"
  class icmp-class
     drop
!
control-plane
 service-policy input control-plane-policy
```

注) CoPP は IOS リリーストレイン 12.0S、12.2S および 12.3T でご利用可能です。 CoPP 機能を設定して使用する際のさらなる以下の URL をご参照ください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a00801afad4.html

2. IPSec で DF bit がセットされている暗号化対象パケットの分割を可能ににします。"crypto ipsec df-bit clear" コマンド （ IOS 12.2(2)T 以降で利用可能 ）または、Policy-Based Routing(PBR) (IOS 12.1(6) 以降で利用可能) によって DF bit を クリアすることによって実現します。

   以下に PBR によって DF bit をクリアする方法を例示します。

```
route-map clear-df permit 10
  match ip address 101
  !--- The following command is used to change the
  !--- Don't Fragment (DF) bit value in the IP header;
  !--- it must be used in route-map configuration mode.
  set ip df 0

access-list 101 permit tcp 10.1.3.0 0.0.0.255 any

interface ethernet0
  ...
  !--- The following command is used to identify a
  !--- route map to use for policy routing on an
  !--- interface; if must be used in interface
  !--- configuration mode.
  ip policy route-map clear-df
```

   この例では、暗号化されていないトラフィックがルータに入るインターフェースに route-map が 適用されており、10.1.3.0/24 が IPSec Tunnel に対するトラフィックの送信元になっています。

Generic Routing Encapsulation(GRE) および IPinIP

この問題に対する唯一の回避策は Tunnel インターフェイスの PMTUD が設定されている場合、それを停止することです。Tunnel インターフェイスの設定モードで "**no tunnel path-mtu-discovery**" によって実現できます。

tunnel path-mtu-discovery コマンドが設定されていない場合、GRE IP ヘッダの DF bit は常にクリアされます。これにより通常は不可能である力プセル化するデータの IP ヘッダに DF bit がセットされている場合でも、 GRE IP パケットの分割が可能となります。

GRE と IPSec と組み合わせて使用している場合、送信パケットの DF bit をクリアにするために

は **crypto ipsec df-bit clear** の代わりに **no tunnel path-mtu-discovery** を使用する必要があります。あわせてルータ宛の ICMP "fragmentation needed and DF bit set" メッセージ（Type 3、Code 4）を Access Control List か Control Plane Policing (CoPP) 機能を使って遮断する必要があります。

Cisco Bug ID CSCef44699（ 登録ユーザのみ)に対する修正を組み込んだイメージをご利用の場合、PMTUD 処理によって学習する最小の MTU を制限すること新規コマンド **tunnel path-mtu-discovery min-mtu<minimum MTU>**が Tunnel インターフェイス設定モードで利用可能です

Layer 2 Tunneling Protocol Version 2(L2TPv2) および Layer 2 Tunneling Protocol Version 3(L2TPv3)

Layer 2 Tunneling Protocol セッション（バージョン 2、 3 とも）を PMTUD 攻撃から 保護する唯一の回避策は PMTUD を停止することです。以下のように L2TPv2 では vpdn-group 設定モードで "no ip pmtu" を設定します

```
router(config)# vpdn enable
router(config)# vpdn-group 1
router(config-vpdn)# no ip pmtu
```

L2TPv3 では以下のように **pseudowire-class** 設定モードで **"no ip pmtu"** および **"no ip dfbit set"** を設定します。

```
pseudowire-class [pseudowire class name]
  encapsulation l2tpv3
  no ip pmtu
  no ip dfbit set
  [...]
```

L2TPv2 に関して、Cisco Bug ID CSCsa52807（登録ユーザーのみ）に対する修正を組み込んだイメージをご利用の場合、PMTUD 処理によって学習する最小および最大の MTU を制限する新規コマンド **vpdn pmtu minimum <minimum MTU>**および **vpdn pmtu maximum <maximum MTU>** が **vpdn-group** 設定モードで利用可能です。

IOS XR の回避策

Cisco CRS-1 が他のピアと TCP 接続を確立している場合は設定による回避策はございません。SMU を適用いただくか、脆弱性が存在しないバージョンの IOS XR にアップグレードをお勧めします。

Cisco IP Phones の回避策

Cisco IP Phone に対する ICMP Hard Error および Source Quench 攻撃に対する 回避策はございません。しかしながら、Voice と Data を VLAN テクノロジーを 活用して分離することで攻撃を緩和することができます。また、 一般的には以下の IP テレフォニーにおいて推奨されるベストプラクティスを 利用して分離することで攻撃の影響を緩和することができます。"SAFE: IP Telephony Security in Depth"

http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a00801b7a50.shtml

Cisco Secure PIX Security Appliance の回避策

該当製品の項の記述の通り、PIX は IPSec が設定されている際にのみ影響を受けます。影響を 受ける場合は（PIX では PMTUD を停止することができないため）回避策がなく脆弱性の存在しない バージョンの PIX ソフトウェアにアップグレードをお勧めします。.

PMTUD 攻撃を回避する方法ではありませんが、 **clear ipsec sa** コマンドによって管理者は Security Association をリセットしトンネルの Path MTU を元の値に回復することができます。

Cisco VPN5000 Concentrator の回避策

PreTunnelFragmentation を「no」に設定することによって PMTUD を停止することが可能です。

VPN 5000 にどのような厳密なアクセス制限を用いても効果はありません。もし、攻撃が外側 (interface Ethernet 1) から生成された場合、それらのパケットは IPSec 接続に対する影響を 与えません。トンネルを経由するものや、内側で生成されたものに関しては PMTUD 攻撃に対して 脆弱性があります。お客様によっては、Ethernet 0 が接続されトンネルを終端している single-arm モードで機器を稼動させている場合があります。この場合、脆弱性がある構成となります。

その他の Operating Systems の回避策

Cisco 製品には Micorosoft Windows や各種 UNIX 上で動作するものがあります。これらの製品は通常、中継装置ではなくエンドホストとして動作します。すなわち、オペレーティングシステムが 脆弱であれば影響を受ける場合があります。本項の回避策、特に PMTUD を停止することはこれらの オペレーティングシステムにとっても有効である場合があります。

Path MTU を Microsoft Windows や各種 UNIX で停止する方法に関する情報は以下が 参考になります。
"Adjusting IP MTU, TCP MSS, and PMTUD on Windows and Sun Systems"

> http://www.cisco.com/en/US/tech/tk870/tk877/tk880/technologies_tech_note09186a008011a218.shtml

ICMP Source Quench 攻撃に対する防御

ICMP "Source Quench" メッセージはネットワーク輻輳の対応としてかつて試みられたものですが、 現在の標準ではこの状況の対応として効果的な方法でないことが認識されています。そのため、現代の TCP/IP の実装において、受信機器はこのメッセージを無視し、また、送信することもありません。以上の状況のため、 脆弱性が存在する機器およびネットワーク境界で ICMP "Source Quench" メッセージを遮断しても比較的安全 であるといえます

詐称されたパケットに対する防御

IP 送信元アドレスを詐称ことによって引き起こされる問題を緩和するのに役立つ Unicast Reverse Path Forwarding (uRPF)、IP source verify、DHCP Lease Query、 AAA を伴う Dynamic ACLs および mini-ACLs（AAA を伴うものも含む）はベストプラクティスとされている一方で、ICMP パケットが詐称されていない攻撃に関しては、攻撃の緩和に効果的でない場合があります。その理由として、 攻撃は必ずしもパケットの詐称を行う必要がないためです。しかしながら、攻撃が詐称パケットによるものであれば、 詐称対策のネットワークエッジにおける適用は攻撃の緩和に役立ちます。

詐称対策に関するさらなる情報は以下をご参照ください。
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml#sec_ip RFC 2827 "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing" http://www.ietf.org/rfc/rfc2827.txt

IOS の Unicast Reverse Path Forwarding (Unicast RPF または uRPF) 機能は 詐称した IP 送信元アドレスによって引き起こされる問題の緩和に有効です。 uRPF を有効にするに以下のコマンドを使用します。

```
router(config)# ip cef
router(config)# interface <interface> <interface #>
router(config-if)# ip verify unicast reverse-path
```

Unicast Reverse Path Fowarding Loose Mode のフィーチャーガイドをご参照いただき具体的な動作や様々な場合の設定方法 については以下をご参照ください。特に非対称ルーティングとなっている場合は重要です。 ftp://ftp-eng.cisco.com/cons/isp/security/URPF-ISP.pdf

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 しておりません。業界全体にわたる本問題に関して NISCC 公開通知を発行しています。 ICMP Source Quench およぼ hard error 問題に関してご報告してくださった、 アルゼンチン国立工科大学の Fernando Gont 氏に謝意を表明します。 Gont 氏の PMTU 問題を含む ICMP による TCP に対するコネクションリセットおよび スループット低下攻撃に関する研究発表資料は以下にてご確認いただけます。 http://www.gont.com.ar/drafts/icmp-attacks-against-tcp.html

この通知のステータス: final

本アドバイザリー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。 本アドバイザリー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。 またシスコシステムズは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-20050412-icmp.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-teams@first.org (includes CERT/CC)
- bugtraq@securityfocus.com
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.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 1.2	2005-April-22	• 以下の製品を「脆弱性が存在しない製品」に追加表記: Cisco 7902/05 and 7920 IP Phones.Cisco LocalDirector. • 以下の製品を「脆弱性が存在する製品」に追加表記: Cisco MGX-8250 and MGX-8850.Cisco Content Switching Module (CSM) - 管理用接続のみ脆弱性が存在。 • Microsoft Security Bulletin MS05-019 . によると Microsoft Windows は PMTUD 攻撃および ICMP "hard error" メッセージによる攻撃に対して脆弱性が存在し、Microsoft Windows ともに出荷された、あるいはその上で動作する全シスコ製品を「脆弱性が存在する製品」 の項に移動。. • 修正 IOS ソフトウェア表の以下のリリースに関する情報の更新: 12.1(23)E4 (12.1(23)E3 で置き換え), 12.1(22)E6, 12.3(11)YF2, 12.3XW, 12.3XS, 12.3XX, 12.3XR, 12.3XQ, 12.3XK, 12.3XE, 12.2EW, 12.2BZ, and 12.3XI. • Cisco MDS9000 に "source quench" に加えて PMTUD 攻撃に対する脆弱性も存在することを追加表記. • GRE、IPinIP および L2TPv2 においては ICMP エラーメッセージの認証が不可能であり、最小 Path MTU を設定する新規コマンドをトンネリングプロトコルに追加した Cisco Bug ID を追加表記. • Conference Bridge および Transcoder/MTP ファームウェアが稼動する 6608 の脆弱性の存在を追加表記. • Cisco PIX Security Appliance: 1) トンネルが PMTUD 攻撃に遭った場合 IPSec トンネルを通過するトラフィックのみが影響を受けることを追加表記。2) PIX Security Appliance ソフトウェアバージョン 7.0 以降は本脆弱性の影響を受けないことを追加表記。3) PMTUD 攻撃の場合 **clear ipsec sa** コマンドで Path MTU を回復できる ことを追加表記。 • PMTUD がデフォルトで停止している

		Cisco-customized Microsoft Windows の最初のバージョンの表記を修正（2000.2.6 に代えて 2000.2.5）。 Cisco MeetingPlace がその OS を使用していることを追加表記。 • Cisco IOS XR ソフトウェアのダウンロードページへのリンクを追加表記。 • IOS XR によいては、ICMP に対する脆弱性の修正に IOS XR のフルアップグレードではなく、SMU も使用できることを強調。 • Cisco IOS で TCP 接続の PMTUD を停止している場合、**ip tcp mss <MSS value>** コマンドは MSS に影響を与えないこと、また、使用される MSS は、接続先がリモートか否かよって 536 バイトもしくはインターフェイス MTU - 40 バイトであると表記。 • GRE を IPSec と組み合わせて使用している場合、送信パケットの DF bit をクリアにするためにコマンド **crypto ipsec df-bit clear** に代えて **no tunnel path-mtu-discovery** を使用すべきであると表記。 • GSS 1.2 以前は影響を受けます。以前は 1.1 以前と表記されておりました。
Revision 1.1	2005-April-12	情報配信の項のメールリストが更新されました。 新しいメールアドレスは以下のとおりです。 full-disclosure@lists.grok.org.uk
Revision 1.0	2005-April-12	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/en/US/products/products_security_vulnerability_policy.html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。