IPv4/IPv6 Dual-stack ルータのための Cisco IOS User Datagram Protocol（UDP）配信問題

High

アドバイザリーID： cisco-sa-20080326-IPv4IPv6

初公開日： 2008-03-26 16:00

バージョン 1.5： Final

CVSSスコア： 7.8

回避策： No Workarounds available

Cisco バグ ID： CSCse56501

CVE-2008-1153

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

有効に なるバージョン 6（IPv6）が Internet Protocol（IP）ある Cisco IOSソフトウェアを実行するデバイスはサービス拒絶（DoS）攻撃に応じてあるかもしれません。 この脆弱性が影響を受けるデバイスに関してはデバイスはまた有効に なるある特定のバージョン 4（IPv4）ユーザ データグラム プロトコル（UDP） サービスが Internet Protocol（IP）なければなりません。 この脆弱性を不正利用するためにおこる IPv6 パケットはデバイスに目標とする必要があります。 ルータ全体ルーティングされるパケットはこの脆弱性を引き起こすことができません。 不正利用の成功はインターフェイスが追加トラフィックを受信することを防ぎます。 唯一の例外は場合不正利用された、デバイスがクラッシュしますリソース予約プロトコル（RSVP）サービスです。 脆弱性が不正利用されたインターフェイスだけ影響を受けています。

Cisco はこの問題に対処するために修正済みソフトウェアを提供しています。 この脆弱性に対しては、影響を緩和するための回避策があります。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-IPv4IPv6 で掲示されます。

注: 2008 年 3月 26 日パブリケーションは 5 つのセキュリティ アドバイザリが含まれています。 アドバイザリはすべて Cisco のインターネットワークオペレーティングシステム（IOS）に影響を与えます。 各アドバイザリはリリースをリストしアドバイザリに説明がある脆弱性を解決するアドバイザリはまたリリースをその正しいすべての 5 つのアドバイザリの脆弱性詳述します。

各ドキュメントへのリンクは次のとおりです。

- Cisco IOS バーチャル プライベート ダイヤルアップ ネットワーク（VPDN） サービス拒否の

脆弱性
326-pptp

- Cisco IOS の多重 DLSw サービス拒否の脆弱性
  326-dlsw
- IPv4/IPv6 Dual-stack ルータのための Cisco IOS User Datagram Protocol（UDP）配信問題
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-IPv4IPv6
- OSPF、MPLS VPN およびスーパバイザ 32、スーパバイザ 720、または Route Switch Processor 720 の Cisco IOS の脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-queue
- Cisco IOS Multicast 仮想 な プライベート ネットワーク（MVPN）データ漏洩
  326-mvpn

該当製品

脆弱性のある製品

有効に なる IPv6 がある Cisco IOS ソフトウェア リリースだけこの脆弱性から影響を受けします。 IPv6 プロトコルのための脆弱 な サポートおよび IPv4 UDP ベース サービス両方であることはデバイスで有効に する必要があります。 IPv6 は Cisco IOSソフトウェアでデフォルトで有効に なりません。

Cisco IOS 製品で実行されているソフトウェアを確認するには、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。 出力次の行で、イメージ名は「バージョンに」先行しているかっこと Cisco IOS ソフトウェアリリース名の間で表示する。 その他の Cisco デバイスには **show version** コマンドがないか、異なる出力が返されます。

次の例は Cisco IOSイメージを実行するデバイスからの出力を示したものです:

```
Router>show version
Cisco IOS Software, 1841 Software (C1841-ADVSECURITYK9-M), Version 12.4(15)T2, RELEASE
SOFTWARE (fc7)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 17-Jan-08 23:12 by prod_rel_team
```

Cisco IOS ソフトウェア リリース指名についてのその他の情報は次のリンクで利用できます: http://www.cisco.com/warp/public/620/1.html。

インターフェイスはのために脆弱 な 2 つの条件で満足しなければなりませんであって下さい:

1. インターフェイスは有効に なる IPv6 がなければなりません。

2. 次の IPv4 UDP ベース サービスの何れか一つ以上は有効に する必要があります:
   TACACS -ポート 49
   ドメイン ネーム システム（DNS） サーバポート 53
   リソース予約プロトコル（RSVP） -ポート 1698
   Layer Two Forwarding（L2F）（L2F)/Layer 2 トンネルプロトコル（L2TP） -ポート 1701
   IP SLA 応答側-ポート 1967
   メディア ゲートウェイ コントロール プロトコル（MGCP） -ポート 2427
   セッション開始プロトコル（SIP） -ポート 5060

他の IPv4 UDP ベース サービスは影響を受けると知られていません。

IPv6 が有効に なるかどうか確認する方法

IPv6 プロトコルはインターフェイスで次の設定行のどちらかまたは両方が設定にある場合有効に なります:

```
Router#show running-config
interface FastEthernet0/1
 ipv6 address 2001:0DB8:C18:1::/64 eui-64
```

```
Router#show running-config
interface FastEthernet0/1
 ipv6 enabled
```

インターフェイスのうちのどれかが **IPv6** 行のどちらかまたは両方が含まれていれば IPv6 はその特定のインターフェイスで有効に なります。

IPv4 UDP ベース サービスが有効に なるかどうか確認する方法

デバイスが影響を受けているかどうか判別するために、デバイスがを受信しているすべての UDP ポートを表示するのに **show ip sockets** コマンドを使用して下さい。 いくつかのより新しい IOS リリースではコマンド **show ip sockets** 廃止 され、代替コマンド **show udp** 代りに使用することができます。 出力は **show ip sockets** コマンドと同じです。

デバイスは **show ip sockets** の出力の**ローカルポート** カラムは（からの第 5 は去りました）下記の例でリストされているのポート番号が含まれている場合脆弱です。

```
Router#show ip sockets
Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
17 192.168.100.1      49 192.168.100.2       49   0   0   11   0
17 0.0.0.0             0 192.168.100.2       53   0   0  211   0
17   --listen--          192.168.100.2     1698   0   0    1   0
17 192.168.100.1    1701 192.168.100.2     1701   1   0 1021   0
17 0.0.0.0             0 192.168.100.2     1967   0   0  211   0
17 0.0.0.0             0  --any--          2427   0   0  211   0
17 0.0.0.0             0  --any--          5060   0   0  211   0
```

脆弱性を含んでいないことが確認された製品

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。

有効に なる IPv6 なしで Cisco IOS を実行するどのデバイスでも脆弱ではないです。 Cisco IOS XR および Cisco PIX/ASA は影響を受けていません。

詳細

この脆弱性を不正利用するためにおこる IPv6 パケットはデバイスに目標とする必要があります。ルータ全体ルーティングされるパケットはこの脆弱性を引き起こすことができません。 脆弱性の不正利用の成功は次の 2 つの状態のいずれかという結果に終るかもしれません:

1. デバイスは RSVP サービスがインターフェイスで設定される場合クラッシュします。
2. インターフェイスが追加トラフィックを受信することを他のどの影響を受けた IPv4 UDP ベース サービスも防ぎます。 脆弱性が不正利用されるインターフェイスだけ影響を受けています。

この脆弱性はインターフェイス メディアタイプの依存しないです。 ブロックされたインターフェイスはすぐに非ブロック化されるまでデバイス自体に向かう後続パケットを受信することを停止します。 デバイスのリロード以外メソッドを使用してインターフェイスを非ブロック化することは可能性のあるです。 これらのメソッドは回避策 セクションに説明があります。 他のインターフェイスはすべて変化しなく、受信および送信パケット続けます。

ブロックされたインターフェイスはトランジットトラフィックがしばらくフローするようにするかもしれません。 トランジットトラフィックはそれぞれルーティングエントリまでフローし続けるかもしれませんまたはアドレス解決プロトコル（ARP） エントリはどのイベントが最初に発生する、切れます。 状況によってはトランジットトラフィックは続ける ARPキャッシュ デフォルトのライフタイムである）数秒以内にブロックされたインターフェイスをフローすることを止めるか、または 4 時間まで（ことができます。 それ以上のトランジットトラフィックがブロックされたインターフェイスをフローしないこと後。

他の IPv4 UDP ベース サービスはこの脆弱性から影響を受けると知られていません。

この脆弱性 Cisco バグ ID CSCse56501 で文書化されています、よくある脆弱性および公開（CVE） ID CVE-2008-1153 は割り当てられました。

脆弱性不正利用の識別

`show interfaces` ブロックされたインプットインターフェイスを識別するために入力キューサイズを表示するのに使用することができます。 攻撃の下のデバイスは、しかしまだブロックされなくてそれに続く低下なしで増加する**入力キューサイズを**示します。 現在のサイズ（この場合、76）最大サイズより大きいです（75）、インプットキューはブロックされます。 75 という値はデフォルト値であり、interface コマンド `hold-queue x` を使用して `in` 変更することができます。

```
Router#show interfaces FastEthernet 0/1 | include queue
  Input queue: 76/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Output queue: 0/40 (size/max)
```

上述の例はインターフェイス FastEthernet0/1 がブロックされることを示します。

show ip sockets コマンドがどのプロトコルがインターフェイスをブロックするか判別するのに使用することができます。 出力のカラムで（からの第 6 は去りま）他のどの数もより含まれていればその特別なプロトコルのパケットはブロックしているというしるしであるゼロ（0）、またはブロックしインターフェイス始めます。 次の例はインターフェイスのインプットキューを一杯にし始めている DNS パケットを示したものです。 インターフェイスは完全に 13 のパケットだけインプットキューにあるのでブロックされません。

```
Router#show ip sockets
Proto    Remote      Port      Local       Port  In Out Stat TTY OutputIF
17 192.168.100.1      49 192.168.100.2       49   0   0   11   0
17 0.0.0.0             0 192.168.100.2       53  13   0  211   0
17   --listen--          192.168.100.2     1698   0   0    1   0
17 192.168.100.1    1701 192.168.100.2     1701   1   0 1021   0
17 0.0.0.0             0 192.168.100.2     1967   0   0  211   0
17 0.0.0.0             0  --any--          2427   0   0  211   0
17 0.0.0.0             0  --any--          5060   0   0  211   0
```

show ip sockets コマンドの出力はインターフェイスで情報を提供しないものです。 マルチプルプロトコルからのパケットが単一 のインターフェイスをブロックするかもしれないことは可能性のあるです。 コマンドの出力はデバイス· コンフィギュレーションと影響を受けたポートを確立するために理解する必要があります。

ブロックされたインターフェイスを検出するのに使用できる追加メソッドは「Cisco に加えました軽減情報を説明があります: User Datagram Protocol（UDP） IPv4/IPv6 Dual-Stack ルータのための配信問題は」
http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20080326-IPv4IPv6 で利用可能文書化します。 メソッドは組み込みイベント マネージャ（EEM）およびアプレットまたは EEM スクリプト利用します。

回避策

インターフェイス アクセス制御リスト

IPv6 Access Control List（ACL）の展開によって脆弱 な UDP サービスに到着する IPv6 パケットをおこらせることを防ぐことは可能性のあるです。 次の例の ACL は達する脆弱 な サービスからのすべての IPv6 トラフィックをブロックします。

```
Router(config)#ipv6 access-list protect_IPv4_services
Router(config-ipv6-acl)#deny udp any 2001:DB8:1:128::/64 eq tacacs
Router(config-ipv6-acl)#deny udp any 2001:DB8:1:128::/64 eq domain
Router(config-ipv6-acl)#deny udp any 2001:DB8:1:128::/64 eq 1698
Router(config-ipv6-acl)#deny udp any 2001:DB8:1:128::/64 eq 1701
```

```
Router(config-ipv6-acl)#deny udp any 2001:DB8:1:128::/64 eq 1967
Router(config-ipv6-acl)#deny udp any 2001:DB8:1:128::/64 eq 2427
Router(config-ipv6-acl)#deny udp any 2001:DB8:1:128::/64 eq 5060
!--- Deny access to link-local address space Router(config-ipv6-acl)#deny udp any FE80::/10 eq
tacacs
Router(config-ipv6-acl)#deny udp any FE80::/10 eq domain
Router(config-ipv6-acl)#deny udp any FE80::/10 eq 1698
Router(config-ipv6-acl)#deny udp any FE80::/10 eq 1701
Router(config-ipv6-acl)#deny udp any FE80::/10 eq 1967
Router(config-ipv6-acl)#deny udp any FE80::/10 eq 2427
Router(config-ipv6-acl)#deny udp any FE80::/10 eq 5060
!--- Permit/deny all other Layer 3 and Layer 4 traffic !--- in accordance with existing security
policies and configurations ! !--- Allow all other IPv6 traffic Router(config-ipv6-acl)#permit
ipv6 any 2001:db8:1:128::/64
! ! Router(config)#interface FastEthernet0/1
Router(config-if)#ipv6 traffic-filter protect_IPv4_services in
```

Receive Access Control List

レシーブ アクセス リスト（rACL）は次のハードウェアモデルで利用可能 な 機能です: Cisco 12000 シリーズ、Cisco 7500 シリーズおよび Cisco 10720 ルータ。

rACL の展開によって IPv6 パケットを達する脆弱 な UDP サービスからおこらせることを防ぐことは可能性のあるです。 次の例の rACL は達する脆弱 な サービスからのすべての IPv6 トラフィックをブロックします。

```
Router(config)#ipv6 access-list protect_IPv4_services
Router(config-ipv6-acl)#deny udp any 2001:DB8:1:128::/64 eq tacacs
Router(config-ipv6-acl)#deny udp any 2001:DB8:1:128::/64 eq domain
Router(config-ipv6-acl)#deny udp any 2001:DB8:1:128::/64 eq 1698
Router(config-ipv6-acl)#deny udp any 2001:DB8:1:128::/64 eq 1701
Router(config-ipv6-acl)#deny udp any 2001:DB8:1:128::/64 eq 1967
Router(config-ipv6-acl)#deny udp any 2001:DB8:1:128::/64 eq 2427
Router(config-ipv6-acl)#deny udp any 2001:DB8:1:128::/64 eq 5060
!--- Deny access to link-local address space Router(config-ipv6-acl)#deny udp any FE80::/10 eq
tacacs
Router(config-ipv6-acl)#deny udp any FE80::/10 eq domain
Router(config-ipv6-acl)#deny udp any FE80::/10 eq 1698
Router(config-ipv6-acl)#deny udp any FE80::/10 eq 1701
Router(config-ipv6-acl)#deny udp any FE80::/10 eq 1967
Router(config-ipv6-acl)#deny udp any FE80::/10 eq 2427
Router(config-ipv6-acl)#deny udp any FE80::/10 eq 5060
!--- Permit/deny all other Layer 3 and Layer 4 traffic !--- in accordance with existing security
policies and configurations ! !--- Allow all other IPv6 traffic Router(config-ipv6-acl)#permit
ipv6 any 2001:db8:1:128::/64
! ! Router(config)#interface FastEthernet0/1
Router(config-if)#ipv6 traffic-filter protect_IPv4_services in
```

追加緩和技術

ネットワーク内の on Cisco 配置されたデバイスの場合もある追加緩和技術はこのアドバイザリに Cisco によって加えられる軽減情報ドキュメントガイドで利用できます:

http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20080326-IPv4IPv6

修正済みソフトウェア

ソフトウェアのアップグレードを検討する際には、http://www.cisco.com/go/psirt およびそれ以降のアドバイザリも参照して、起こりうる障害と完全なアップグレード ソリューションを判断してください

いずれの場合も、アップグレードする機器に十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新しいリリースで引き続き適切にサポートされていることの確認を十分に行ってください。 情報に不明な点がある場合は、Cisco Technical Assistance Center（TAC）または契約を結んでいるメンテナンス プロバイダーにお問い合せください。

Cisco IOS ソフトウェアの表（下掲）の各行には、Cisco IOS のリリース トレインが記載されています。 特定のリリース トレインに脆弱性がある場合は、修正を含む最初のリリース（および、それぞれの予想提供日）が表の「第 1 修正済みリリース」列に記載されます。 「推奨リリース」列には、このアドバイザリが作成された時点で発表されているすべての脆弱性の修正を含むリリースが記載されます。 特定の列に記されているリリースよりも古い（第 1 修正済みリリースより古い）トレインに含まれるリリースが稼働しているデバイスは脆弱であることが確認されています。 表の「推奨リリース」列に記載されているリリース、またはそれよりも新しいリリースにアップグレードすることを推奨します。

メジャー リリース	修正済みリリースの入手可能性	
Affected 12.0-Based Releases	First Fixed Release（修正された最初のリリース）	**推奨リリース**
12.0	脆弱性なし	
12.0DA	脆弱性なし	
12.0DB	脆弱性なし	
12.0DC	脆弱性なし	
12.0S	脆弱性あり; contact TAC	
12.0SC	脆弱性なし	
12.0SL	脆弱性なし	
12.0SP	脆弱性なし	
12.0ST	脆弱性なし	
12.0SX	脆弱性なし	
12.0SY	脆弱性あり; contact TAC	
12.0SZ	脆弱性あり; contact TAC	
12.0T	脆弱性なし	
12.0W	脆弱性なし	

12.0WC	脆弱性なし	
12.0WT	脆弱性なし	
12.0XA	脆弱性なし	
12.0XB	脆弱性なし	
12.0XC	脆弱性なし	
12.0XD	脆弱性なし	
12.0XE	脆弱性なし	
12.0XF	脆弱性なし	
12.0XG	脆弱性なし	
12.0XH	脆弱性なし	
12.0XI	脆弱性なし	
12.0XJ	脆弱性なし	
12.0XK	脆弱性なし	
12.0XL	脆弱性なし	
12.0XM	脆弱性なし	
12.0XN	脆弱性なし	
12.0XQ	脆弱性なし	
12.0XR	脆弱性なし	
12.0XS	脆弱性なし	
12.0XV	脆弱性なし	
12.0XW	脆弱性なし	
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**
12.1	脆弱性なし	
12.1AA	脆弱性なし	
12.1AX	脆弱性なし	
12.1AY	脆弱性なし	
12.1AZ	脆弱性なし	
12.1CX	脆弱性なし	
12.1DA	脆弱性なし	
12.1DB	脆弱性なし	
12.1DC	脆弱性なし	
12.1E	脆弱性なし	
12.1EA	脆弱性なし	
12.1EB	脆弱性なし	
12.1EC	脆弱性なし	
12.1EO	脆弱性なし	
12.1EU	脆弱性なし	
12.1EV	脆弱性なし	
12.1EW	脆弱性なし	

12.1EX	脆弱性なし	
12.1EY	脆弱性なし	
12.1EZ	脆弱性なし	
12.1GA	脆弱性なし	
12.1GB	脆弱性なし	
12.1T	脆弱性なし	
12.1XA	脆弱性なし	
12.1XB	脆弱性なし	
12.1XC	脆弱性なし	
12.1XD	脆弱性なし	
12.1XE	脆弱性なし	
12.1XF	脆弱性なし	
12.1XG	脆弱性なし	
12.1XH	脆弱性なし	
12.1XI	脆弱性なし	
12.1XJ	脆弱性なし	
12.1XK	脆弱性なし	
12.1XL	脆弱性なし	
12.1XM	脆弱性なし	
12.1XN	脆弱性なし	
12.1XO	脆弱性なし	
12.1XP	脆弱性なし	
12.1XQ	脆弱性なし	
12.1XR	脆弱性なし	
12.1XS	脆弱性なし	
12.1XT	脆弱性なし	
12.1XU	脆弱性あり; first fixed in 12.3	12.3(26)
12.1XV	脆弱性あり; first fixed in 12.3	12.3(26)
12.1XW	脆弱性なし	
12.1XX	脆弱性なし	
12.1XY	脆弱性なし	
12.1XZ	脆弱性なし	
12.1YA	脆弱性なし	
12.1YB	脆弱性あり; first fixed in 12.3	12.3(26)
12.1YC	脆弱性あり; first fixed in 12.3	12.3(26)
12.1YD	脆弱性あり; first fixed in 12.3	12.3(26)
12.1YE	Release prior to 12.1(5)YE6 are vulnerable， releases 12.1(5)YE6 and later are not vulnerable; first fixed in 12.3	12.3(26)
12.1YF	脆弱性あり; first fixed in 12.3	12.3(26)
12.1YG	脆弱性なし	
12.1YH	脆弱性あり; first fixed in 12.3	12.3(26)

12.1YI	脆弱性あり; first fixed in 12.3	12.3(26)
12.1YJ	脆弱性なし	
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**
12.2	脆弱性なし	
12.2B	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2BC	脆弱性あり; first fixed in 12.3BC	12.3(23)BC1
12.2BW	脆弱性あり; first fixed in 12.3	12.3(26)
12.2BY	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2BZ	脆弱性あり; first fixed in 12.3XI	
12.2CX	脆弱性あり; first fixed in 12.3BC	12.3(23)BC1
12.2CY	脆弱性あり; first fixed in 12.3BC	12.3(23)BC1
12.2CZ	脆弱性あり; contact TAC	
12.2DA	脆弱性なし	
12.2DD	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2DX	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2EU	脆弱性あり; first fixed in 12.2SG	12.2(25)EWA13 12.2(31)SGA5 12.2(44)SG
12.2EW	脆弱性あり; first fixed in 12.2SG	12.2(25)EWA13 12.2(31)SGA5 12.2(44)SG
12.2EWA	12.2(25)EWA10 12.2(25)EWA11	12.2(25)EWA13
12.2EX	12.2(35)EX1 12.2(37)EX	12.2(40)EX1
12.2EY	12.2(37)EY	
12.2EZ	脆弱性あり; first fixed in 12.2SEE	
12.2FX	脆弱性あり; first fixed in 12.2SEE	
12.2FY	脆弱性あり; first fixed in 12.2SEG	12.2(25)SEG4
12.2FZ	脆弱性あり; first fixed in 12.2SE	12.2(44)SE1
12.2IXA	脆弱性あり; contact TAC	
12.2IXB	脆弱性あり; contact TAC	

12.2IXC	脆弱性あり; contact TAC	
12.2IXD	脆弱性あり; contact TAC	
12.2IXE	脆弱性なし	
12.2JA	脆弱性あり; first fixed in 12.3JA	
12.2JK	脆弱性あり; first fixed in 12.4T	12.4(15)T4
12.2MB	脆弱性あり; contact TAC	
12.2MC	12.2(15)MC2h	12.2(15)MC2k
12.2S	12.2(14)S18 12.2(18)S13 12.2(20)S14 12.2(25)S13	12.2(25)S15
12.2SB	12.2(28)SB7 12.2(31)SB5 12.2(33)SB; 31-MAR-2008 で利用可能	12.2(31)SB11
12.2SBC	脆弱性あり; first fixed in 12.2SB; 31-MAR-2008 で利用可能	12.2(31)SB11
12.2SCA	脆弱性なし	
12.2SE	12.2(35)SE4 12.2(37)SE	12.2(44)SE1
12.2SEA	脆弱性あり; first fixed in 12.2SEE	
12.2SEB	脆弱性あり; first fixed in 12.2SEE	
12.2SEC	脆弱性あり; first fixed in 12.2SEE	
12.2SED	脆弱性あり; first fixed in 12.2SEE	
12.2SEE	12.2(25)SEE4	
12.2SEF	12.2(25)SEF3	12.2(44)SE1
12.2SEG	12.2(25)SEG3	12.2(25)SEG4
12.2SG	12.2(25)SG3 12.2(31)SG3 12.2(37)SG	12.2(44)SG
12.2SGA	12.2(31)SGA2 12.2(31)SGA3 12.2(31)SGA6; 07-APR-2008 で利用可能	12.2(31)SGA5
12.2SL	脆弱性なし	
12.2SM	脆弱性あり; contact TAC	
12.2SO	脆弱性あり; migrate to any release in 12.2SVA	12.2(29)SVD
12.2SRA	12.2(33)SRA4	12.2(33)SRA7
12.2SRB	12.2(33)SRB1	12.2(33)SRB3; 14-APR-08 で利用可能

12.2SRC	脆弱性なし	
12.2SU	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2SV	12.2(29b)SV	12.2(29b)SV
12.2SVA	脆弱性なし	
12.2SVC	脆弱性なし	
12.2SVD	脆弱性なし	
12.2SW	脆弱性あり; contact TAC	
12.2SX	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF13
12.2SXA	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF13
12.2SXB	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF13
12.2SXD	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF13
12.2SXE	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF13
12.2SXF	12.2(18)SXF10a 12.2(18)SXF12a 12.2(18)SXF9	12.2(18)SXF13
12.2SXH	脆弱性なし	
12.2SY	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF13
12.2SZ	脆弱性あり; first fixed in 12.2S	12.2(25)S15 12.2(31)SB11 12.2(33)SRC
12.2T	脆弱性あり; first fixed in 12.3	12.3(26)
12.2TPC	12.2(8)TPC10b	
12.2UZ	脆弱性あり; first fixed in 12.2SB; 31-MAR-2008 で利用可能	12.2(31)SB11
12.2XA	脆弱性あり; first fixed in 12.3	12.3(26)
12.2XB	脆弱性あり; first fixed in 12.3	12.3(26)
12.2XC	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2XD	脆弱性あり; first fixed in 12.3	12.3(26)
12.2XE	脆弱性あり; first fixed in 12.3	12.3(26)
12.2XF	脆弱性あり; first fixed in 12.3BC	12.3(23)BC1
12.2XG	脆弱性あり; first fixed in 12.3	12.3(26)
12.2XH	脆弱性あり; first fixed in 12.3	12.3(26)
12.2XI	脆弱性あり; first fixed in 12.3	12.3(26)
12.2XJ	脆弱性あり; first fixed in 12.3	12.3(26)
12.2XK	脆弱性あり; first fixed in 12.3	12.3(26)

12.2XL	脆弱性あり; first fixed in 12.3	12.3(26)
12.2XM	脆弱性あり; first fixed in 12.3	12.3(26)
12.2XN	12.2(33)XN1	12.3(26)
12.2XO	脆弱性なし	
12.2XQ	脆弱性あり; first fixed in 12.3	12.3(26)
12.2XR	脆弱性あり; first fixed in 12.3	12.3(26)
12.2XS	脆弱性なし	
12.2XT	脆弱性あり; first fixed in 12.3	12.3(26)
12.2XU	脆弱性あり; first fixed in 12.3	12.3(26)
12.2XV	脆弱性あり; first fixed in 12.3	12.3(26)
12.2XW	脆弱性あり; first fixed in 12.3	12.3(26)
12.2YA	12.2(4)YA13; 31-MAR-2008 で利用可能	12.3(26)
12.2YB	脆弱性あり; first fixed in 12.3	12.3(26)
12.2YC	脆弱性あり; first fixed in 12.3	12.3(26)
12.2YD	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2YE	脆弱性あり; first fixed in 12.2S	12.2(25)S15 12.2(31)SB11 12.2(33)SRC
12.2YF	脆弱性あり; first fixed in 12.3	12.3(26)
12.2YG	脆弱性あり; first fixed in 12.3	12.3(26)
12.2YH	脆弱性あり; first fixed in 12.3	12.3(26)
12.2YJ	脆弱性あり; first fixed in 12.3	12.3(26)
12.2YK	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2YL	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2YM	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2YN	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2YO	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF13
12.2YP	脆弱性あり; first fixed in 12.3	12.3(26)
12.2YQ	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2YR	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2YS	脆弱性なし	
12.2YT	脆弱性あり; first fixed in 12.3	12.3(26)
12.2YU	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2YV	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2YW	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2YX	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2YY	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2YZ	脆弱性あり; first fixed in 12.2S	12.2(25)S15

		12.2(31)SB11 12.2(33)SRC
12.2ZA	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF13
12.2ZB	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2ZC	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2ZD	脆弱性あり; contact TAC	
12.2ZE	脆弱性あり; first fixed in 12.3	12.3(26)
12.2ZF	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2ZG	脆弱性あり; first fixed in 12.3YG	12.4(15)T4 12.4(18a)
12.2ZH	12.2(13)ZH9	12.2(13)ZH11
12.2ZJ	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2ZL	脆弱性あり; first fixed in 12.4	12.4(15)T4 12.4(18a)
12.2ZP	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2ZU	脆弱性あり; migrate to any release in 12.2SXH	12.2(33)SXH2
12.2ZY	脆弱性なし	
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**
12.3	12.3(17c) 12.3(18a) 12.3(19a) 12.3(23)	12.3(26)
12.3B	脆弱性あり; first fixed in 12.4	12.4(18a)
12.3BC	12.3(17b)BC8 12.3(21a)BC2 12.3(23)BC	12.3(23)BC1
12.3BW	脆弱性あり; first fixed in 12.4	12.4(18a)
12.3EU	脆弱性なし	
12.3JA	12.3(11)JA4 12.3(7)JA5	
12.3JEA	12.3(8)JEA2	12.3(8)JEA4
12.3JEB	12.3(8)JEB1	12.3(8)JEB2
12.3JEC	脆弱性なし	
12.3JK	12.3(2)JK3 12.3(8)JK	12.3(8)JK1
12.3JL	12.3(2)JL2	12.3(2)JL4

12.3JX	12.3(7)JX9	12.3(7)JX10
12.3T	脆弱性あり; first fixed in 12.4	12.4(18a)
12.3TPC	12.3(4)TPC11b	
12.3VA	脆弱性あり; contact TAC	
12.3XA	12.3(2)XA6	12.3(2)XA7; 31-MAR-08 で利用可能
12.3XB	脆弱性あり; first fixed in 12.4	12.4(18a)
12.3XC	12.3(2)XC5	12.4(15)T4 12.4(18a)
12.3XD	脆弱性あり; first fixed in 12.4	12.4(18a)
12.3XE	12.3(2)XE6; 31-MAR-2008 で利用可能	12.4(15)T4 12.4(18a)
12.3XF	脆弱性あり; first fixed in 12.4	12.4(18a)
12.3XG	脆弱性あり; first fixed in 12.3YG	12.4(15)T4 12.4(18a)
12.3XH	脆弱性あり; first fixed in 12.4	12.4(18a)
12.3XI	12.3(7)XI10	
12.3XJ	脆弱性あり; first fixed in 12.3YX	12.3(14)YX11 12.4(15)T4
12.3XK	脆弱性あり; first fixed in 12.4	12.4(18a)
12.3XQ	脆弱性あり; first fixed in 12.4	12.4(18a)
12.3XR	12.3(7)XR7	12.3(7)XR8; 31-MAR-08 で利用可能
12.3XS	脆弱性あり; first fixed in 12.4	12.4(18a)
12.3XU	脆弱性あり; first fixed in 12.4T	12.4(15)T4
12.3XW	脆弱性あり; first fixed in 12.3YX	12.3(14)YX11 12.4(15)T4
12.3XY	脆弱性あり; first fixed in 12.4	12.4(18a)
12.3YA	脆弱性あり; first fixed in 12.4	12.4(15)T4 12.4(18a)
12.3YD	脆弱性あり; first fixed in 12.4T	12.4(15)T4
12.3YF	脆弱性あり; first fixed in 12.3YX	12.3(14)YX11 12.4(15)T4
12.3YG	12.3(8)YG6	12.4(15)T4
12.3YH	脆弱性あり; first fixed in 12.4T	12.4(15)T4
12.3YI	脆弱性あり; first fixed in 12.4T	12.4(15)T4
12.3YJ	脆弱性あり; first fixed in 12.4T	12.4(15)T4
12.3YK	12.3(11)YK3	12.4(15)T4

12.3YM	12.3(14)YM10	12.3(14)YM12
12.3YQ	脆弱性あり; first fixed in 12.4T	12.4(15)T4
12.3YS	12.3(11)YS3; 31-MAR-2008 で利用可能	12.4(15)T4
12.3YT	脆弱性あり; first fixed in 12.4T	12.4(15)T4
12.3YU	脆弱性あり; first fixed in 12.4XB	
12.3YX	12.3(14)YX8	12.3(14)YX11
12.3YZ	12.3(11)YZ2	
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	12.4(10c) 12.4(12) 12.4(3h) 12.4(5c) 12.4(7e) 12.4(8d)	12.4(18a)
12.4JA	脆弱性なし	
12.4JK	脆弱性なし	
12.4JMA	脆弱性なし	
12.4JMB	脆弱性なし	
12.4JMC	脆弱性なし	
12.4JX	脆弱性なし	
12.4MD	脆弱性なし	
12.4MR	12.4(12)MR	12.4(16)MR2
12.4SW	12.4(11)SW3	12.4(15)SW
12.4T	12.4(11)T2 12.4(15)T 12.4(2)T6 12.4(4)T8 12.4(6)T8 12.4(9)T3	12.4(15)T4
12.4XA	脆弱性あり; first fixed in 12.4T	12.4(15)T4
12.4XB	12.4(2)XB6	
12.4XC	12.4(4)XC7	
12.4XD	12.4(4)XD7	12.4(4)XD10
12.4XE	12.4(6)XE2	12.4(15)T4
12.4XF	脆弱性なし	
12.4XG	12.4(9)XG2	12.4(9)XG2

12.4XJ	12.4(11)XJ4	12.4(15)T4
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	
12.4XT	12.4(6)XT1	12.4(6)XT2
12.4XV	脆弱性なし	
12.4XW	脆弱性なし	
12.4XY	脆弱性なし	

不正利用事例と公式発表

Cisco PSIRT はこのアドバイザリに記載される脆弱性の公示か不正利用に気づいていません。

この脆弱性はカスタマーネットワークで見つけられました。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-IPv4IPv6

改訂履歴

Revision 1.5	2008-June-27	リンクおよび冗漫を取除く更新済要約。
リビジョン 1.4	2008-April-25	CSCse56501 への更新済 CVSS リンク。
リビジョン 1.3	2008-April-14	リンク ローカル アドレス空間は回避策 セクションの iACL 例に入ります
リビジョン 1.2	2008-April-01	Ciscoルータ 12000 のための rACL を使用する追加された対応策、7500 および 10720 シリーズ。
リビジョン 1.1	2008-Mar-29	advisory ID cisco-sa-20080326-IPv4IPv6 の新しい情報による 12.0S、12.0SY、12.0SX および 12.0SZ のための更新済ソフトウェア テーブル IPv4IPv6 デュアルスタック ルータの行進第 26 アドバイザリ。
リビジョ	2008-Mar-	初版リリース

ン 1.0	26	

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。