Cisco 10000、uBR10012、uBR7200 シリーズ デバイス IPC 脆弱性

High

アドバイザリーID : cisco-sa-20080924-ipc
初公開日 : 2008-09-24 16:00
バージョン 1.1 : Final
CVSSスコア : 8.5
回避策 : Yes
Cisco バグ ID : CSCsg15342 , CSCsh29217

CVE-2008-3805
CVE-2008-3806

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

Cisco 10000 は、uBR10012 および uBR7200 シリーズ デバイス ユーザ データグラム プロトコル（UDP）によって基づく Inter-Process Communication （IPC） チャネルを使用します外部に到達可能である。 攻撃者により影響を受けたデバイスのサービス拒否 （DoS）条件を引き起こすのにこの脆弱性を不正利用する可能性があります。 他のプラットフォームは影響を受けていません。

シスコはこの脆弱性に対処するソフトウェア アップデートをリリースしました。 この脆弱性を軽減する回避策は利用できます。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ipc で掲示されます。

注: 2008 年 9月 24 日 IOS アドバイザリによって組み込まれる書は 12 のセキュリティ アドバイザリが含まれています。 アドバイザリの 11 は Cisco の IOS software の脆弱性に対処し、1 つのアドバイザリは Cisco Unified Communications Manager の脆弱性に対処します。 各アドバイザリはリリースをリストしますアドバイザリに説明がある脆弱性を解決する。

各ドキュメントへのリンクは次のとおりです。

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-iosips
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-sip
- 924-cucm

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-vpn
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-mfi
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ubr
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-multicast
- 924-sccp
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-iosfw
- 924-l2tp

影響を受ける製品

Cisco 10000 は、Cisco IOS の影響を受けたバージョンを実行している uBR10012 および uBR7200 シリーズ デバイス影響を受けています。

脆弱性が存在する製品

Cisco IOS を実行しているデバイスは **show version コマンドの**使用によって識別することができます。 次の例は Cisco IOS ソフトウェア リリース 12.2(31)SB10e を実行する Cisco 10000 シリーズ デバイスから奪取 される出力を示したものです:

```
c10k#show version | include IOS Cisco IOS Software, 10000 Software (C10K3-P11-M), Version
12.2(31)SB10e, RELEASE SOFTWARE (fc1) c10k#
```

次の例は Cisco IOS ソフトウェア リリース 12.3(17b)BC7 を実行する Cisco uBR10012 シリーズ デバイスから奪取 される出力を示したものです:

```
ubr10k#show version | include IOS IOS (tm) 10000 Software (UBR10K-K8P6U2-M), Version
12.3(17b)BC7, RELEASE SOFTWARE (fc1) ubr10k#
```

次の例は Cisco IOS ソフトウェア リリース 12.3(21a)BC2 を実行する Cisco uBR7200 シリーズ デバイスから奪取 される出力を示したものです:

```
ubr7200#show version | include IOS IOS (tm) 7200 Software (UBR7200-IK9SU2-M), Version
12.3(21a)BC2, RELEASE SOFTWARE (fc1) ubr7200#
```

「白書と資格を与えられる文書を参照して下さい: Cisco IOSリリース命名規則のその他の情報のための Cisco IOSレファレンスガイド」。 このドキュメントは、次のリンクで入手できます。 http://www.cisco.com/warp/public/620/1.html

ソフトウェア バージョン および 修正 下記の例にリストされている修正済み バージョン前の Cisco IOS のどのバージョンでも脆弱です。

脆弱性が存在しない製品

Cisco uBR7100 シリーズ デバイスは影響を受けていません。

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

細部

Cisco 10000 は、uBR10012 および uBR7200 シリーズ デバイス UDP ベース IPC チャネルを使用します。 このチャネルは 127.0.0.0/8 範囲および UDP ポート 1975 からのアドレスを使います。 Cisco 10000 は、Cisco IOS の影響を受けたバージョンを実行している uBR10012 および uBR7200 シリーズ デバイス デバイスのの外からの UDP ポート 1975 に送られる IPC メッセージを処理します。 攻撃者によってこの動作が DoS 状態に終ってデバイスか、ラインカード、またはその両方のリロードを、引き起こすのに不正利用されるかもしれません。

127.0.0.0/8 に向かう不正 な トラフィックか UDP ポート 1975 をフィルタリングしてこの脆弱性を軽減します。

この脆弱性 Cisco バグ ID CSCsg15342 （登録ユーザのみ）および CSCsh29217 （登録ユーザのみ）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-2008-3805 は割り当てられました。

回避策

回避策はフィルタリングパケットでポート 1975 に送信される UDP パケットおよび 127.0.0.0/8 範囲に送信される構成されています。

インターフェイスの使用アクセス コントロール リスト（ACL）

ポート 1975 に向かう UDP パケットをフィルタリングするアクセス リストがこの脆弱性を軽減するのに使用することができます。 UDP ポート 1975 はある特定のアプリケーションによって使用できる登録済みのポート番号です。 ただし、UDP ポート 1975 に向かうすべてのパケットをフィルタリングするによりいくつかのアプリケーションは故障しますかもしれません。 従って、アクセス リストは明示的に ルータ インターフェイス IP アドレスおよび割り当てトランジットトラフィックに送信される UDP 1975 パケットを拒否する必要があります。 そのようなアクセス リストは有効であるためにすべてのインターフェイスで追加される必要があります。 IPC チャネルが 127.0.0.0/8 範囲からのアドレスを使うので、ソースをたどられるか、またはこの範囲に向かわれるパケットをフィルタリングすることもまた必要です。 例は下記のように与えられます:

```
access-list 100 deny udp any host <router-interface 1> eq 1975
access-list 100 deny udp any host <router-interface 2> eq 1975
access-list 100 deny udp any host <router-interface ...> eq 1975
access-list 100 deny ip 127.0.0.0 0.255.255.255 any
access-list 100 deny ip any 127.0.0.0 0.255.255.255
access-list 100 permit ip any any

interface Serial 0/0
  ip access-group 100 in
```

コントロール プレーン ポリシングの使用

コントロール プレーン ポリシング（CoPP）が影響を受けたデバイスに信頼できない UDP ポー

ト 1975 アクセスをブロックするのに使用することができます。 Cisco IOS ソフトウェア リリース 12.2BC および 12.2SCA は CoPP 機能をサポートします。 デバイスに CoPP を設定して、管理プレーンとコントロール プレーンを保護し、既存のセキュリティ ポリシーおよび設定に従って、インフラストラクチャのデバイスに送信される承認されたトラフィックだけを明示的に許可することで、インフラストラクチャへの直接攻撃のリスクと効果を最小限に抑えることができます。 次の例をネットワークに適用できます。

注： CoPP は uBR10012 シリーズ デバイスでサポートされません。

```
!-- Permit all UDP/1975 traffic so that it !-- will be policed and dropped by the CoPP feature !
access-list 111 permit udp any any eq 1975 access-list 111 permit ip any 127.0.0.0 0.255.255.255
access-list 111 permit ip 127.0.0.0 0.255.255.255 any ! !-- Permit (Police or Drop)/Deny (Allow)
all other Layer 3 and !-- Layer 4 traffic in accordance with existing security policies !-- and
configurations for traffic that is authorized to be sent !-- to infrastructure devices ! !--
Create a Class-Map for traffic to be policed by the CoPP !-- feature ! class-map match-all drop-
IPC-class match access-group 111 ! !-- Create a Policy-Map that will be applied to the Control-
Plane !-- of the device ! policy-map drop-IPC-traffic class drop-IPC-class drop ! !-- Apply the
Policy-Map to the Control-Plane of the device ! control-plane service-policy input drop-IPC-
traffic !
```

CoPP 上の例では、「拒否」操作を一致するパケットは policy-map ドロップする 機能から（示されていない）影響を受けないが policy-map 「ドロップする」機能によって廃棄されるこれらのパケットの「割り当て」アクションの結果を用いる潜在的なエクスプロイト パケットを一致する アクセス制御リスト エントリ（ACE）。

以下の事項に注意して下さい: Cisco IOS 12.2S および 12.0S で policy-map 構文を異なっていますトレインします:

```
!
policy-map drop-IPC-traffic class drop-IPC-class
  police 32000 1500 1500 conform-action drop exceed-action drop
!
```

CoPP 機能の設定および使用のその他の情報は http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html、http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.html および http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html で見つけることができます。

ネットワーク境界のインフラストラクチャ ACL の使用

ネットワークを移動するトラフィックをブロックするのは往々にして困難ですが、インフラストラクチャ デバイスに送られてはならないトラフィックを識別し、ネットワークの境界でそのトラフィックをブロックすることは可能です。 iACLs はネットワーク セキュリティ 最良 の 方法で、よいネットワーク セキュリティへの長期付加、またこの特定の脆弱性のための回避策として考慮する必要があります。 下記に示されている iACL 例はインフラストラクチャ IPアドレス範囲の IP アドレスのすべてのデバイスを保護するかどれが展開されたインフラストラクチャ access-list の一部として含まれるはずです:

```
!-- Note: IPC packets sent to UDP destination port 1975 must not !-- be permitted from any
trusted source as this traffic !-- should only be sent and received internally by the !--
affected device using an IP address allocated from the !-- 127.0.0.0/8 prefix. !-- !-- IPC that
traffic that is internally generated and sent !-- and/or received by the affected device is not
subjected !-- to packet filtering by the applied iACL policy. ! !-- Deny IPC (UDP port 1975)
packets from all sources destined to !-- all IP addresses configured on the affected device. !
access-list 150 deny udp any host INTERFACE_ADDRESS#1 eq 1975 access-list 150 deny udp any host
INTERFACE_ADDRESS#2 eq 1975 access-list 150 deny udp any host INTERFACE_ADDRESS#N eq 1975 ! !--
Deny all IP packets with a source or destination IP address !-- from the 127.0.0.0/8 prefix. !
access-list 150 deny ip 127.0.0.0 0.255.255.255 any access-list 150 deny ip any 127.0.0.0
0.255.255.255 ! !-- Permit/deny all other Layer 3 and Layer 4 traffic in accordance !-- with
existing security policies and configurations. ! !-- Permit all other traffic to transit the
device. ! access-list 150 permit ip any any ! !-- Apply iACL to interfaces in the ingress
direction. ! interface GigabitEthernet0/0 ip access-group 150 in !
```

注： ポート 1975 に向かう UDP パケットをフィルタリングする iACLs がこの脆弱性を軽減するのに使用することができます。 ただし、UDP ポート 1975 はある特定のアプリケーションによって使用できる登録済みのポート番号です。 UDP ポート 1975 に向かうすべてのパケットをフィルタリングするによりいくつかのアプリケーションは故障しますかもしれません。 従って次に、明示的に影響を受けたデバイス、そして割り当てのためのあらゆるルータ インターフェイス IP アドレスにおよび/または他のレイヤ3 およびレイヤ4 トラフィックをすべて既存 の セキュリティポリシーおよびコンフィギュレーションに従って拒否するために送信されるデバイスを通過する 1975 年の宛先ポート、および割り当てを使用して UDP パケットを拒否する iACL ポリシー必要他のすべてのトラフィック。 iACLs は効果的に使用されるべきすべてのインターフェイスで加える必要があります。 IPC チャネルが 127.0.0.0/8 範囲からのアドレスを使うので、ソースをたどられるか、または前述の例のこの範囲にそのまま向かわれるパケットをフィルタリングすることもまた必要です。

ホワイトペーパー 『Protecting Your Core: Infrastructure Protection Access Control Lists (ACL) には、インフラストラクチャ保護アクセス リストに関するガイドラインと推奨配備方法が記載されています。 この White Paper は次のサイトで提供されています。

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

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次のリンクで利用可能の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-20080924-ipc-and-ubr

固定ソフトウェア

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	Release prior to 12.0(32)S are vulnerable， releases 12.0(32)S and later are not vulnerable;	12.0(32)S11 12.0(33)S1
12.0SC	脆弱性なし	
12.0SL	、移行する 12.0S に脆弱、12.1	
12.0SP	脆弱性なし	
12.0ST	、移行する 12.0S に脆弱、12.1	
12.0SX	脆弱性なし	
12.0SY	脆弱性なし	
12.0SZ	12.0(30)SZ4	12.0(32)S11 12.0(33)S1
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	
12.0XT	脆弱性なし	
12.0XV	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**
該当する 12.1 ベースのリリースはありません。		
Affected 12.2-Based Releases	First Fixed Release (修正された最初のリリース)	**推奨リリース**
12.2	脆弱性なし	
12.2B	脆弱性なし	
12.2BC	脆弱性なし	
12.2BW	脆弱性なし	
12.2BX	脆弱性なし	
12.2BY	脆弱性なし	
12.2BZ	脆弱性なし	
12.2CX	脆弱性なし	
12.2CY	脆弱性なし	
12.2CZ	脆弱性なし	
12.2DA	脆弱性なし	
12.2DD	脆弱性なし	
12.2DX	脆弱性なし	
12.2EW	脆弱性なし	
12.2EWA	脆弱性なし	
12.2EX	脆弱性なし	
12.2EY	脆弱性なし	
12.2EZ	脆弱性なし	
12.2FX	脆弱性なし	
12.2FY	脆弱性なし	

12.2FZ	脆弱性なし	
12.2IRB	脆弱性なし	
12.2IXA	脆弱性なし	
12.2IXB	脆弱性なし	
12.2IXC	脆弱性なし	
12.2IXD	脆弱性なし	
12.2IXE	脆弱性なし	
12.2IXF	脆弱性なし	
12.2IXG	脆弱性なし	
12.2JA	脆弱性なし	
12.2JK	脆弱性なし	
12.2MB	脆弱性なし	
12.2MC	脆弱性なし	
12.2S	脆弱性なし	
12.2SB	12.2(31)SB13 12.2(33)SB1	12.2(33)SB2; 26-SEP-08 で利用可能
12.2SBC	脆弱性なし	
12.2SCA	12.2(33)SCA1	12.2(33)SCA1
12.2SE	脆弱性なし	
12.2SEA	脆弱性なし	
12.2SEB	脆弱性なし	
12.2SEC	脆弱性なし	
12.2SED	脆弱性なし	
12.2SEE	脆弱性なし	
12.2SEF	脆弱性なし	
12.2SEG	脆弱性なし	
12.2SG	脆弱性なし	
12.2SGA	脆弱性なし	
12.2SL	脆弱性なし	
12.2SM	脆弱性なし	
12.2SO	脆弱性なし	
12.2SRA	脆弱性なし	
12.2SRB	脆弱性なし	
12.2SRC	12.2(33)SRC2	12.2(33)SRC2
12.2SU	脆弱性なし	
12.2SV	脆弱性なし	
12.2SVA	脆弱性なし	
12.2SVC	脆弱性なし	
12.2SVD	脆弱性なし	

12.2SW	脆弱性なし	
12.2SX	脆弱性なし	
12.2SXA	脆弱性なし	
12.2SXB	脆弱性なし	
12.2SXD	脆弱性なし	
12.2SXE	脆弱性なし	
12.2SXF	脆弱性なし	
12.2SXH	脆弱性なし	
12.2SY	脆弱性なし	
12.2SZ	脆弱性なし	
12.2T	脆弱性なし	
12.2TPC	脆弱性なし	
12.2XA	脆弱性なし	
12.2XB	脆弱性なし	
12.2XC	脆弱性なし	
12.2XD	脆弱性なし	
12.2XE	脆弱性なし	
12.2XF	脆弱性なし	
12.2XG	脆弱性なし	
12.2XH	脆弱性なし	
12.2XI	脆弱性なし	
12.2XJ	脆弱性なし	
12.2XK	脆弱性なし	
12.2XL	脆弱性なし	
12.2XM	脆弱性なし	
12.2XN	脆弱性なし	
12.2XNA	脆弱性なし	
12.2XNB	脆弱性なし	
12.2XO	脆弱性なし	
12.2XQ	脆弱性なし	
12.2XR	脆弱性なし	
12.2XS	脆弱性なし	
12.2XT	脆弱性なし	
12.2XU	脆弱性なし	
12.2XV	脆弱性なし	
12.2XW	脆弱性なし	
12.2YA	脆弱性なし	
12.2YB	脆弱性なし	
12.2YC	脆弱性なし	
12.2YD	脆弱性なし	
12.2YE	脆弱性なし	
12.2YF	脆弱性なし	

12.2YG	脆弱性なし	
12.2YH	脆弱性なし	
12.2YJ	脆弱性なし	
12.2YK	脆弱性なし	
12.2YL	脆弱性なし	
12.2YM	脆弱性なし	
12.2YN	脆弱性なし	
12.2YO	脆弱性なし	
12.2YP	脆弱性なし	
12.2YQ	脆弱性なし	
12.2YR	脆弱性なし	
12.2YS	脆弱性なし	
12.2YT	脆弱性なし	
12.2YU	脆弱性なし	
12.2YV	脆弱性なし	
12.2YW	脆弱性なし	
12.2YX	脆弱性なし	
12.2YY	脆弱性なし	
12.2YZ	脆弱性なし	
12.2ZA	脆弱性なし	
12.2ZB	脆弱性なし	
12.2ZC	脆弱性なし	
12.2ZD	脆弱性なし	
12.2ZE	脆弱性なし	
12.2ZF	脆弱性なし	
12.2ZG	脆弱性なし	
12.2ZH	脆弱性なし	
12.2ZJ	脆弱性なし	
12.2ZL	脆弱性なし	
12.2ZP	脆弱性なし	
12.2ZU	脆弱性なし	
12.2ZX	脆弱性あり; first fixed in 12.2SB	12.2(33)SB2; 26-SEP-08 で利用可能
12.2ZY	脆弱性なし	
12.2ZYA	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	脆弱性なし	
12.3B	脆弱性なし	
12.3BC	12.3(17b)BC6	12.3(23)BC

	12.3(21a)BC1 12.3(23)BC	4
12.3BW	脆弱性なし	
12.3EU	脆弱性なし	
12.3JA	脆弱性なし	
12.3JEA	脆弱性なし	
12.3JEB	脆弱性なし	
12.3JEC	脆弱性なし	
12.3JK	脆弱性なし	
12.3JL	脆弱性なし	
12.3JX	脆弱性なし	
12.3T	注： Release prior to 12.3(14)T3 are vulnerable， releases 12.3(14)T3 and later are not vulnerable;	12.4(15)T7 12.4(18c)
12.3TPC	脆弱性なし	
12.3VA	脆弱性なし	
12.3XA	脆弱性なし	
12.3XB	脆弱性なし	
12.3XC	脆弱性なし	
12.3XD	脆弱性なし	
12.3XE	脆弱性なし	
12.3XF	脆弱性なし	
12.3XG	脆弱性なし	
12.3XI	12.3(7)XI10a	12.2(33)SB2; 26-SEP-08 で利用可能
12.3XJ	脆弱性なし	
12.3XK	脆弱性なし	
12.3XL	脆弱性なし	
12.3XQ	脆弱性なし	
12.3XR	脆弱性なし	
12.3XS	脆弱性なし	
12.3XU	脆弱性なし	
12.3XW	脆弱性なし	
12.3XX	脆弱性なし	
12.3XY	脆弱性なし	
12.3XZ	脆弱性なし	
12.3YA	脆弱性なし	
12.3YD	脆弱性なし	
12.3YF	脆弱性なし	
12.3YG	脆弱性なし	
12.3YH	脆弱性なし	

12.3YI	脆弱性なし	
12.3YJ	脆弱性なし	
12.3YK	脆弱性なし	
12.3YM	脆弱性なし	
12.3YQ	脆弱性なし	
12.3YS	脆弱性なし	
12.3YT	脆弱性なし	
12.3YU	脆弱性なし	
12.3YX	脆弱性なし	
12.3YZ	脆弱性なし	
12.3ZA	脆弱性なし	
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	注： Release prior to 12.4(3) are vulnerable， releases 12.4(3) and later are not vulnerable;	12.4(18c)
12.4JA	脆弱性なし	
12.4JK	脆弱性なし	
12.4JL	脆弱性なし	
12.4JMA	脆弱性なし	
12.4JMB	脆弱性なし	
12.4JMC	脆弱性なし	
12.4JX	脆弱性なし	
12.4MD	脆弱性なし	
12.4MR	脆弱性なし	
12.4SW	脆弱性なし	
12.4T	脆弱性なし	
12.4XA	脆弱性なし	
12.4XB	脆弱性なし	
12.4XC	脆弱性なし	
12.4XD	脆弱性なし	
12.4XE	脆弱性なし	
12.4XF	脆弱性なし	
12.4XG	脆弱性なし	
12.4XJ	脆弱性なし	
12.4XK	脆弱性なし	
12.4XL	脆弱性なし	
12.4XM	脆弱性なし	
12.4XN	脆弱性なし	
12.4XP	脆弱性なし	
12.4XQ	脆弱性なし	

12.4XR	脆弱性なし	
12.4XT	脆弱性なし	
12.4XV	脆弱性なし	
12.4XW	脆弱性なし	
12.4XY	脆弱性なし	
12.4XZ	脆弱性なし	
12.4YA	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 Cisco 内部で発見されたものです。

ソース

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ipc

改訂履歴

リビジョン 1.1	2009-April-16	現在旧式であるように、結合されたソフトウェア テーブルへの取除かれた参照
リビジョン 1.0	2008-Sep-24	初回公開リリース

利用規約