Cisco IOSソフトウェアの複数のマルチキャスト脆弱性

High

アドバイザリーID : cisco-sa-20080924-multicast
初公開日 : 2008-09-24 16:00
バージョン 1.3 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID : CSCsl34355 CSCsd95616

CVE-2008-3808
CVE-2008-3809

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

2 細工 された Protocol Independent Multicast （ PIM ）パケットの脆弱性はサービス拒否（ DoS ）に状態を導くかもしれない Cisco IOSソフトウェアにあります。 シスコはこれらの脆弱性に対処するソフトウェア アップデートを提供しています。 これらの脆弱性に対しては回避策があります。

このアドバイザリは http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-multicast 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-ipc
- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ubr

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

該当製品

脆弱性のある製品

Cisco IOSソフトウェアを実行している PIM のために設定されて特別に 巧妙に細工された PIM パケットに関する脆弱性があり、デバイスに。 さらに、Cisco IOSソフトウェアを実行している Cisco 12000 シリーズ（GSR）ルータに巧妙に細工された マルチキャスト パケットに関する 2つめの脆弱性があります。

show running-config | ip pim コマンドを Cisco IOSデバイスが PIM のために設定されることを確認するために発行することができます**含んで下さい**。 次の例では、Cisco IOS ルータは PIM 希薄-稠密 モードのために設定されます。

```
Router#show running-config | include ip pim
 ip pim sparse-dense-mode
```

Cisco IOSデバイスの利用可能 な PIM モードが稠密モード、希薄モード、または希薄-稠密 モードであることに注目して下さい。 これらのモードの何れかのために設定されるデバイスはこれらの脆弱性から影響を受けます。 モードはデバイスがマルチキャストルーティングテーブルをどのように読み込む、そしてどのようにマルチキャスト パケットが転送されるか判別します。 PIM は少なくとも 1 インターフェイスのこれらのモードの 1 つで有効に する デバイスが IPマルチキャストルーティングを処理することができるように必要があります。 デフォルトモード 設定がありません。 マルチキャストルーティングはデフォルトでディセーブルにされます。 ただし、Cisco IOSデバイスは少なくとも 1 つのインターフェイスが PIM のために設定される場合脆弱です。

さらに、Protocol Independent Multicast （PIM）のために設定されるインターフェイスについての情報を表示するために次の例に示すようにユーザか特権EXECモードで EXEC **show ip pim interface コマンドを**、使用して下さい:

```
Router# show ip pim interface

Address          Interface                Ver/   Nbr    Query  DR     DR
                                          Mode   Count  Intvl  Prior

10.1.0.1         GigabitEthernet0/0       v2/SD  0      30     1      10.1.0.1
10.6.0.1         GigabitEthernet0/1       v2/SD  1      30     1      10.6.0.2
```

ソフトウェアを判別するためにデバイスに Cisco IOS 製品で、ログイン動作するシステムバナーを表示する show version コマンドを発行すれば。 Cisco IOSソフトウェアは「インターネットワーク オペレーティング システム ソフトウェア」として識別しますそれ自身をまたは単に「IOS」。 出力次の行、「バージョンに」先行しているかっこと Cisco IOS リリース名前間の

イメージ名 ディスプレイ。 他の Ciscoデバイスに show version コマンドがありませんし、別の出力を与えないために。

次の例は 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 ip pim interface

Address          Interface                Ver/   Nbr    Query  DR     DR
                                          Mode   Count  Intvl  Prior

10.1.0.1         GigabitEthernet0/0       v2/SD  0      30     1      10.1.0.1
10.6.0.1         GigabitEthernet0/1       v2/SD  1      30     1      10.6.0.2
```

脆弱性を含んでいないことが確認された製品

PIM のために設定されない Cisco IOSデバイスは脆弱ではないです。 Cisco IOS XR ソフトウェアはこの脆弱性から影響を受けません。 他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

詳細

2 細工 された Protocol Independent Multicast （PIM）パケットの脆弱性はサービス拒否（DoS）に状態を導くかもしれない Cisco IOSソフトウェアにあります。 Cisco IOSソフトウェアを実行し、PIM のために設定されるデバイスは最初の脆弱性から影響を受けます。 PIM のために設定される Cisco 12000 シリーズ（GSR）ルータだけ 2つめの脆弱性から影響を受けます。

Cisco IOSデバイスの利用可能 な PIM モードは稠密モード、希薄モード、または希薄-稠密 モードです。 モードはデバイスがマルチキャストルーティングテーブルをどのように読み込む、そしてどのようにマルチキャスト パケットが転送されるか判別します。 PIM は少なくとも 1 インターフェイスのこれらのモードの 1 つで有効に する デバイスが IPマルチキャストルーティングを処理することができるように必要があります。

注: デフォルトモード 設定がありません。 マルチキャストルーティングはデフォルトでディセーブルにされます。 ただし、Cisco IOSデバイスは少なくとも 1 つのインターフェイスが PIM のために設定される場合脆弱です。

インターフェイスの PIM を稠密モードにあるために設定するためにインターフェイス設定モードで次のコマンドを使用して下さい:

```
Router(config-if)# ip pim dense-mode
```

インターフェイスの PIM を希薄モードにあるために設定するためにインターフェイス設定モードで次のコマンドを使用して下さい:

```
Router(config-if)# ip pim sparse-mode
```

インターフェイスの PIM を希薄-稠密 モードにあるために設定するためにインターフェイス設定モードで次のコマンドを使用して下さい:

```
Router(config-if)# ip pim sparse-dense-mode
```

これらの脆弱性は次の Cisco バグ ID で文書化されています:

- CSCsd95616 -巧妙に細工された PIM パケットにより IOSデバイスはリロードしますかもしれません
- CSCsl34355 - GSR は不正 な マルチキャスト パケットを処理するときクラッシュするかもしれません

これらの脆弱性よくある脆弱性および公開（CVE）識別 CVE-2008-3808 および CVE-2008-3809 は割り当てられました。

回避策

2つめの脆弱性のための回避策がありません。 次の回避策は Cisco バグ ID CSCsd95616 で当たる脆弱性にだけ適用されます。 PIM ルータは PIM 隣接性を確立するために PIM Hellos を受け取る必要があります。 PIM 隣接性はまた Designated Router （DR）選択、DR フェールオーバー、および/PIM 加入/Prune を/アサート 送信 するのための基礎受諾メッセージです。 規定 するために PIM 隣接を、使用します次の例に示すように **ip pim neighbor-filter コマンドを**、信頼しました:

```
Router(config)#access-list 1 permit host 10.10.10.123
!-- An access control list is created to allow a trusted PIM neighbor !-- in this example the
neighbor is 10.10.10.123 ! Router(config)#interface fastEthernet 0/0
Router(config-if)#ip pim neighbor-filter 1
!-- The PIM neighbor filter is then applied to the respective interface(s)
```

ip pim neighbor-filter コマンドは Hellos、加入/Prune、および BSR パケットを含む信頼できないデバイスからの PIM パケットをフィルタリングします。

注: この文書に説明がある脆弱性はスプーフィングされたIP パケットによって攻撃者が **ip pim neighbor-filter** 実装にリストされている信頼された PIM 相手の IP アドレスを知っている場合不正利用することができます。

インフラストラクチャ デバイスを保護し、リスクを、直接インフラストラクチャ不正侵入の影響最小限に抑えるためにおよび効果は、管理者 コア インフラストラクチャ 機器に送信 される トラフィックのポリシー施行を行うために ACL を展開するように助言されます。 PIM は IP プロトコル 103 です。 追加回避策として、管理者は割り当て承認された PIM だけ明示的にできます（IP プロトコル 103）トラフィックは既存 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インフラストラクチャ デバイスに送信 しました。 ACL は次の例に示すように展開することができます:

```
Router(config)#access-list 1 permit host 10.10.10.123
!-- An access control list is created to allow a trusted PIM neighbor !-- in this example the
neighbor is 10.10.10.123 ! Router(config)#interface fastEthernet 0/0
Router(config-if)#ip pim neighbor-filter 1
!-- The PIM neighbor filter is then applied to the respective interface(s)
```

Cisco 機器に適用可能な追加の軽減策については以下の "Cisco Applied Intelligence companion document" より入手可能です。
http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20080924-multicast。

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	修理されたリリースの Â Â Â Â Â 可用性	
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	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0DA	Release prior to 12.0(8)DA3 are vulnerable， releases 12.0(8)DA3 and later are not vulnerable; first fixed in 12.2DA	12.2(12)DA13 12.4(15)T7 12.4(18c)

12.0DB	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0DC	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0S	12.0(32)S8 12.0(33)S	12.0(32)S11 12.0(33)S1
12.0SC	脆弱性あり; first fixed in 12.0S	12.0(32)S11 12.0(33)S1
12.0SL	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0SP	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0ST	脆弱性あり; first fixed in 12.0S	12.0(32)S11 12.0(33)S1
12.0SX	脆弱性あり; first fixed in 12.0S	12.0(32)S11 12.0(33)S1
12.0SY	12.0(32)SY5	12.0(32)SY7; 29-SEP-08 で利用可能
12.0SZ	12.0(30)SZ4	12.0(32)S11 12.0(33)S1
12.0T	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0W	脆弱性あり; first fixed in 12.2	12.0(3c)W5(8)
12.0WC	Release prior to 12.0(5)WC10 are vulnerable， releases 12.0(5)WC10 and later are not vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0WT	脆弱性なし	
12.0XA	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)

12.0XB	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XC	Release prior to 12.0(2)XC2 are vulnerable， releases 12.0(2)XC2 and later are not vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XD	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XE	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XF	脆弱性なし	
12.0XG	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XH	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XI	Release prior to 12.0(4)XI2 are vulnerable， releases 12.0(4)XI2 and later are not vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XJ	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XK	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XL	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XM	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XN	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XQ	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XR	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.0XS	脆弱性なし	
12.0XT	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)

12.0XV	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
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	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1AA	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1AX	脆弱性あり; first fixed in 12.2EY	12.2(46)SE
12.1AY	Release prior to 12.1(22)AY1 are vulnerable， releases 12.1(22)AY1 and later are not vulnerable; first fixed in 12.1EA	12.1(22)EA12 12.2(46)SE
12.1AZ	脆弱性なし	
12.1CX	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1DA	脆弱性あり; first fixed in 12.2DA	12.2(12)DA13 12.4(15)T7 12.4(18c)
12.1DB	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1DC	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1E	12.1(27b)E2	12.2(18)SXF15
12.1EA	12.1(22)EA10	12.1(22)EA12
12.1EB	脆弱性あり; contact TAC	
12.1EC	脆弱性あり; first fixed in 12.3BC	12.2(33)SCA1 12.3(23)BC4
12.1EO	脆弱性あり; first fixed in 12.2SV	
12.1EU	脆弱性あり; first fixed in 12.2EWA	12.2(25)EWA14 12.2(31)SGA8

		12.2(46)SG1
12.1EV	脆弱性なし	
12.1EW	脆弱性あり; first fixed in 12.2	12.2(25)EWA14 12.2(31)SGA8 12.2(46)SG1 12.4(15)T7 12.4(18c)
12.1EX	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1EY	脆弱性あり; contact TAC	
12.1EZ	脆弱性あり; first fixed in 12.1E	12.2(18)SXF15 12.4(15)T7 12.4(18c)
12.1GA	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1GB	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1T	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XA	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XB	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XC	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XD	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XE	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XF	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1XG	脆弱性あり; first fixed in 12.2	12.4(15)T

		7 12.4(18c)
12.1XH	脆弱性あり; first fixed in 12.2	12.4(15)T 7 12.4(18c)
12.1XI	脆弱性あり; first fixed in 12.2	12.4(15)T 7 12.4(18c)
12.1XJ	脆弱性あり; first fixed in 12.2	12.4(15)T 7 12.4(18c)
12.1XL	脆弱性あり; first fixed in 12.2	12.4(15)T 7 12.4(18c)
12.1XM	脆弱性あり; first fixed in 12.2	12.4(15)T 7 12.4(18c)
12.1XP	脆弱性あり; first fixed in 12.2	12.4(15)T 7 12.4(18c)
12.1XQ	脆弱性あり; first fixed in 12.2	12.4(15)T 7 12.4(18c)
12.1XR	脆弱性あり; first fixed in 12.2	12.4(15)T 7 12.4(18c)
12.1XS	脆弱性あり; first fixed in 12.2	12.4(15)T 7 12.4(18c)
12.1XT	脆弱性あり; first fixed in 12.2	12.4(15)T 7 12.4(18c)
12.1XU	脆弱性あり; first fixed in 12.2	12.4(15)T 7 12.4(18c)
12.1XV	脆弱性あり; first fixed in 12.2	12.4(15)T 7 12.4(18c)
12.1XW	脆弱性あり; first fixed in 12.2	12.4(15)T 7 12.4(18c)
12.1XX	脆弱性あり; first fixed in 12.2	12.4(15)T 7 12.4(18c)
12.1XY	脆弱性あり; first fixed in 12.2	12.4(15)T 7 12.4(18c)
12.1XZ	脆弱性あり; first fixed in 12.2	12.4(15)T 7

		12.4(18c)
12.1YA	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1YB	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1YC	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1YD	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1YE	Release prior to 12.1(5)YE6 are vulnerable， releases 12.1(5)YE6 and later are not vulnerable; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1YF	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1YH	脆弱性あり; first fixed in 12.2	12.4(15)T7 12.4(18c)
12.1YI	脆弱性あり; contact TAC	
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	12.2(26c) 12.2(27c) 12.2(28d) 12.2(29b) 12.2(46)	12.4(15)T7 12.4(18c)
12.2B	脆弱性あり; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2BC	脆弱性あり; first fixed in 12.3	12.2(33)SCA1 12.3(23)BC4 12.4(15)T7 12.4(18c)
12.2BW	脆弱性あり; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2BX	脆弱性あり; first fixed in 12.3	12.2(33)S

		B2; 26-SEP-08 で利用可能 12.4(15)T7 12.4(18c)
12.2BY	脆弱性あり; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2BZ	脆弱性あり; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2CX	脆弱性あり; first fixed in 12.3	12.2(33)SCA1 12.3(23)BC4 12.4(15)T7 12.4(18c)
12.2CY	脆弱性あり; first fixed in 12.3	12.2(33)SCA1 12.3(23)BC4 12.4(15)T7 12.4(18c)
12.2CZ	脆弱性あり; first fixed in 12.2S	12.2(33)SB2; 26-SEP-08 で利用可能
12.2DA	12.2(10)DA9 12.2(12)DA13	12.2(12)DA13
12.2DD	脆弱性あり; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2DX	脆弱性あり; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2EW	脆弱性あり; first fixed in 12.2EWA	12.2(25)EWA14 12.2(31)SGA8 12.2(46)SG1
12.2EWA	12.2(25)EWA10 12.2(25)EWA11	12.2(25)EWA14
12.2EX	12.2(37)EX	12.2(35)EX2
12.2EY	12.2(37)EY	
12.2EZ	脆弱性あり; first fixed in 12.2SEE	12.2(46)S

		E
12.2FX	脆弱性なし	
12.2FY	脆弱性なし	
12.2FZ	脆弱性あり; first fixed in 12.2SE	12.2(46)SE
12.2IRB	脆弱性なし	
12.2IXA	脆弱性あり; migrate to any release in 12.2IXE	12.2(18)IXG
12.2IXB	脆弱性あり; migrate to any release in 12.2IXE	12.2(18)IXG
12.2IXC	脆弱性あり; migrate to any release in 12.2IXE	12.2(18)IXG
12.2IXD	脆弱性あり; migrate to any release in 12.2IXE	12.2(18)IXG
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	脆弱性あり; first fixed in 12.2SW	12.2(25)SW12 12.4(15)T7 12.4(18c)
12.2MC	12.2(15)MC2i	12.4(15)T7 12.4(18c)
12.2S	12.2(14)S18 12.2(18)S13 12.2(20)S13 12.2(25)S13	12.2(33)SB2; 26-SEP-08 で利用可能
12.2SB	12.2(28)SB7 12.2(31)SB5 12.2(33)SB	12.2(33)SB2; 26-SEP-08 で利用可能
12.2SBC	脆弱性あり; first fixed in 12.2SB	12.2(33)SB2; 26-SEP-08 で利用可能
12.2SCA	脆弱性なし	
12.2SE	12.2(35)SE4 12.2(37)SE	12.2(46)SE
12.2SEA	脆弱性あり; first fixed in 12.2SEE	12.2(46)SE
12.2SEB	脆弱性あり; first fixed in 12.2SEE	12.2(46)SE

12.2SEC	脆弱性あり; first fixed in 12.2SEE	12.2(46)SE
12.2SED	脆弱性あり; first fixed in 12.2SEE	12.2(46)SE
12.2SEE	12.2(25)SEE4	12.2(46)SE
12.2SEF	脆弱性なし	
12.2SEG	12.2(25)SEG3	12.2(25)SEG6
12.2SG	12.2(25)SG3 12.2(31)SG3 12.2(37)SG	12.2(46)SG1
12.2SGA	12.2(31)SGA2	12.2(31)SGA8
12.2SL	脆弱性なし	
12.2SM	12.2(29)SM3	12.2(29)SM4
12.2SO	脆弱性あり; first fixed in 12.2SV	
12.2SRA	12.2(33)SRA4	12.2(33)SRB4 12.2(33)SRC2
12.2SRB	脆弱性なし	
12.2SRC	脆弱性なし	
12.2SU	脆弱性あり; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.2SV	12.2(29b)SV1	
12.2SVA	脆弱性なし	
12.2SVC	脆弱性なし	
12.2SVD	脆弱性なし	
12.2SW	12.2(25)SW12	12.2(25)SW12
12.2SX	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF15
12.2SXA	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF15
12.2SXB	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF15
12.2SXD	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF15
12.2SXE	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF15

12.2SXF	12.2(18)SXF9	12.2(18)SXF15
12.2SXH	脆弱性なし	
12.2SY	脆弱性あり; first fixed in 12.2S	12.2(33)SB2; 26-SEP-08 で利用可能
12.2SZ	脆弱性あり; first fixed in 12.2S	12.2(33)SB2; 26-SEP-08 で利用可能
12.2T	脆弱性あり; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2TPC	脆弱性あり; contact TAC	
12.2XA	脆弱性あり; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2XB	脆弱性あり; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2XC	脆弱性あり; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2XD	脆弱性あり; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2XE	脆弱性あり; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2XF	脆弱性あり; first fixed in 12.3	12.2(33)SCA1 12.3(23)BC4 12.4(15)T7 12.4(18c)
12.2XG	Release prior to 12.2(2)XG1 are vulnerable， releases 12.2(2)XG1 and later are not vulnerable; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2XH	脆弱性あり; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2XI	脆弱性あり; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2XJ	脆弱性あり; first fixed in 12.3	12.4(15)T

		7 12.4(18c)
12.2XK	脆弱性あり; first fixed in 12.3	12.4(15)T 7 12.4(18c)
12.2XL	脆弱性あり; first fixed in 12.3	12.4(15)T 7 12.4(18c)
12.2XM	脆弱性あり; first fixed in 12.3	12.4(15)T 7 12.4(18c)
12.2XN	12.2(33)XN1	12.2(33)S B2; 26- SEP-08 で 利用可能 12.2(33)S RC2 12.2(33)X NA2
12.2XN A	脆弱性なし	
12.2XN B	脆弱性なし	
12.2XO	脆弱性なし	
12.2XQ	脆弱性あり; first fixed in 12.3	12.4(15)T 7 12.4(18c)
12.2XR	Release prior to 12.2(15)XR are vulnerable ， releases 12.2(15)XR and later are not vulnerable; first fixed in 12.3	12.3(8)JE A3 12.4(15)T 7 12.4(18c)
12.2XS	脆弱性あり; first fixed in 12.3	12.4(15)T 7 12.4(18c)
12.2XT	脆弱性あり; first fixed in 12.3	12.4(15)T 7 12.4(18c)
12.2XU	脆弱性あり; first fixed in 12.3	12.4(15)T 7 12.4(18c)
12.2XV	脆弱性あり; first fixed in 12.3	12.4(15)T 7 12.4(18c)
12.2XW	脆弱性あり; first fixed in 12.3	12.4(15)T 7 12.4(18c)
12.2YA	脆弱性あり; first fixed in 12.3	12.4(15)T 7

		12.4(18c)
12.2YB	脆弱性あり; contact TAC	
12.2YC	脆弱性あり; contact TAC	
12.2YD	脆弱性あり; contact TAC	
12.2YE	脆弱性あり; contact TAC	
12.2YF	脆弱性あり; contact TAC	
12.2YG	脆弱性あり; contact TAC	
12.2YH	脆弱性あり; contact TAC	
12.2YJ	脆弱性あり; contact TAC	
12.2YK	脆弱性あり; contact TAC	
12.2YL	脆弱性あり; contact TAC	
12.2YM	脆弱性あり; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.2YN	脆弱性あり; contact TAC	
12.2YO	脆弱性あり; contact TAC	
12.2YP	脆弱性あり; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2YQ	脆弱性あり; contact TAC	
12.2YR	脆弱性あり; contact TAC	
12.2YS	脆弱性なし	
12.2YT	脆弱性あり; contact TAC	
12.2YU	脆弱性あり; contact TAC	
12.2YV	脆弱性あり; contact TAC	
12.2YW	脆弱性あり; contact TAC	
12.2YX	脆弱性あり; contact TAC	
12.2YY	脆弱性あり; contact TAC	
12.2YZ	脆弱性あり; contact TAC	
12.2ZA	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF15
12.2ZB	脆弱性あり; contact TAC	
12.2ZC	脆弱性あり; contact TAC	
12.2ZD	脆弱性あり; contact TAC	
12.2ZE	脆弱性あり; first fixed in 12.3	12.4(15)T7 12.4(18c)
12.2ZF	脆弱性あり; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.2ZG	脆弱性あり; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.2ZH	12.2(13)ZH9	12.4(15)T7

		12.4(18c)
12.2ZJ	脆弱性あり; contact TAC	
12.2ZL	脆弱性あり; contact TAC	
12.2ZP	脆弱性あり; contact TAC	
12.2ZU	脆弱性あり; migrate to any release in 12.2SXH	12.2(33)SXH3
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	12.3(17c) 12.3(18a) 12.3(19a) 12.3(20a) 12.3(21)	12.4(15)T7 12.4(18c)
12.3B	脆弱性あり; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.3BC	12.3(17b)BC6 12.3(21)BC	12.3(23)BC4
12.3BW	脆弱性あり; first fixed in 12.4	12.4(15)T7 12.4(18c)
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	脆弱性あり; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.3TPC	脆弱性あり; contact TAC	
12.3VA	脆弱性なし	
12.3XA	12.3(2)XA7	12.4(15)T7 12.4(18c)
12.3XB	脆弱性あり; contact TAC	

12.3XC	脆弱性あり; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.3XD	脆弱性あり; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.3XE	脆弱性あり; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.3XF	脆弱性あり; contact TAC	
12.3XG	脆弱性あり; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.3XI	12.3(7)XI10	12.2(33)SB2; 26-SEP-08 で利用可能
12.3XJ	脆弱性あり; first fixed in 12.3YX	12.3(14)YX13 12.4(15)T7
12.3XK	脆弱性あり; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.3XL	脆弱性あり; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.3XQ	脆弱性あり; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.3XR	12.3(7)XR7	12.4(15)T7 12.4(18c)
12.3XS	脆弱性あり; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.3XU	脆弱性あり; first fixed in 12.4T	12.4(15)T7
12.3XW	脆弱性あり; first fixed in 12.3YX	12.3(14)YX13 12.4(15)T7
12.3XX	12.3(8)XX2d	12.4(15)T7 12.4(18c)
12.3XY	脆弱性あり; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.3XZ	脆弱性あり; first fixed in 12.4	12.4(15)T

		7 12.4(18c)
12.3YA	脆弱性あり; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.3YD	脆弱性あり; first fixed in 12.4T	12.4(15)T7
12.3YF	脆弱性あり; first fixed in 12.3YX	12.3(14)YX13 12.4(15)T7
12.3YG	12.3(8)YG6	12.4(15)T7
12.3YH	脆弱性あり; first fixed in 12.4T	12.4(15)T7
12.3YI	脆弱性あり; first fixed in 12.4T	12.4(15)T7
12.3YJ	脆弱性あり; first fixed in 12.4T	12.4(15)T7
12.3YK	脆弱性あり; first fixed in 12.4T	12.4(15)T7
12.3YM	12.3(14)YM10	12.3(14)YM13; 30-SEP-08 で利用可能
12.3YQ	脆弱性あり; first fixed in 12.4T	12.4(15)T7
12.3YS	脆弱性あり; first fixed in 12.4T	12.4(15)T7
12.3YT	脆弱性あり; first fixed in 12.4T	12.4(15)T7
12.3YU	脆弱性あり; first fixed in 12.4XB	12.4(2)XB10 12.4(9)XG3 12.4(15)T7
12.3YX	12.3(14)YX8	12.3(14)YX13
12.3YZ	12.3(11)YZ3	
12.3ZA	脆弱性あり; first fixed in 12.4T	12.4(15)T7
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(18c)

	12.4(12) 12.4(3h) 12.4(5c) 12.4(7e) 12.4(8d)	
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	12.4(11)MR	12.4(19)MR
12.4SW	脆弱性なし	
12.4T	12.4(11)T 12.4(2)T6 12.4(4)T8 12.4(6)T7 12.4(9)T3	12.4(15)T7
12.4XA	脆弱性あり; first fixed in 12.4T	12.4(15)T7
12.4XB	12.4(2)XB6	12.4(2)XB10
12.4XC	脆弱性あり; first fixed in 12.4T	12.4(15)T7
12.4XD	12.4(4)XD8	12.4(4)XD11; 26-SEP-08 で利用可能
12.4XE	脆弱性あり; first fixed in 12.4T	12.4(15)T7
12.4XF	脆弱性なし	
12.4XG	12.4(9)XG2	12.4(9)XG3
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	脆弱性あり; contact TAC	
12.4XQ	脆弱性なし	
12.4XR	脆弱性なし	
12.4XT	12.4(6)XT2	12.4(15)T

		7
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

このアドバイザリで説明されている脆弱性の公表や悪用に関する情報は Cisco PSIRT には寄せられていません。

これらの脆弱性は内部テストで発見されました。

出典

URL

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

改訂履歴

リビジョン 1.3	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 1.2	2008-October-14	回避策 情報 アップデート。
リビジョン 1.1	2008-September-27	少なくとも 1 つのインターフェイスが PIM のために設定される場合 Cisco IOSデバイスが脆弱であること明白にして下さい。
リビジョン 1.0	2008-September-24	初版リリース

利用規約