Cisco IOS Multicast 仮想 な プライベート ネットワーク（MVPN）データ漏洩

High

アドバイザリーID : cisco-sa-20080326-mvpn

初公開日 : 2008-03-26 16:00

バージョン 1.3 : Final

CVSSスコア : 7.5

回避策 : No Workarounds available

Cisco バグ ID : CSCsi01470

CVE-2008-1156

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

マルチキャスト 仮想 な プライベート ネットワーク（MVPN）の Ciscoインプリメンテーションの脆弱性は悪意のあるユーザがコア ルータの余分マルチキャスト状態を作成するか、または特別に 巧妙に細工された メッセージの送信によって他のマルチプロトコル ラベル スイッチング（MPLS）によって基づくバーチャル プライベート ネットワーク（VPN）からマルチキャストトラフィックを受信することを可能にすることができる不正利用に応じてあります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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 326-mvpn 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 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

Cisco IOS を実行し、MVPN のために設定されるデバイスは影響を受けています。

MVPN のために設定される IOSデバイスは実行コンフィギュレーション例でこれに類似したである行を備えています:

```
mdt default <group-address>
```

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 version
    Cisco IOS Software, 7200 Software (C7200-IK9S-M), Version 12.3(14)T1, RELEASE SOFTWARE
(fc1)
    Technical Support: http://www.cisco.com/techsupport
    Copyright (c) 1986-2005 by Cisco Systems, Inc.
    Compiled Thu 31-Mar-05 08:04 by yiyan
```

Cisco IOS ソフトウェア リリースの命名方法に関する詳細については、次のリンクを参照してください。 http://www.cisco.com/warp/public/620/1.html。

脆弱性を含んでいないことが確認された製品

その他のCisco製品は、IOS XR ソフトウェアを含んで、現在この脆弱性から影響を受けるために知られていません。

詳細

MPLS VPN のマルチキャストトラフィックをサポートすることをサービス プロバイダーが可能にするのを助ける手順および MVPN アーキテクチャは追加一組のプロトコルを導入します。 MVPN はプロバイダの MPLS VPN バックボーンを渡る IP マルチキャスト トラフィックの透過的な転送するを可能にし、サービス プロバイダーが MPLS VPN 顧客にマルチキャストサービスを提供することを可能にします。

攻撃者が余分マルチキャストの作成を引き起こす場合がある特別に 巧妙に細工された マルチキャスト配布ツリー（MDT）データ 加入 メッセージを送信 することを可能にする MVPN の実装で存在 する脆弱性はコア ルータで示します。 MDT データ 加入 メッセージはユニキャストかマルチキャストで送信 することができます。 脆弱性はまた別の MPLS VPNs からのマルチキャストトラフィックをリークさせることを割り当てることができます。 同じ Provider Edge（PE）ルータに接続されない VPN からマルチキャストトラフィックを受信することは可能性のあるです。 正常にこの脆弱性を不正利用するために、攻撃者はリモート PE ルータのボーダー ゲートウェイ プロトコル（BGP）ピアリング IP アドレスおよび他の MPLS VPNs で使用するマルチキャストグループのアドレスを認識するか、または推測する必要があります。

この脆弱性 Cisco バグ ID CSCsi01470（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-2008-1156 は割り当てられました。

回避策

この脆弱性のための回避策は PE デバイスの MDT データ 加入パケットのフィルタリングで構成されています。

回避策はすべての PE ルータのすべてのバーチャルルーティングおよびフォワーディング（VRF）インターフェイスで適用される必要があります。 さもなければ、攻撃者はリモート PE ルータをターゲットとし、まだこの脆弱性を不正利用できます。

ネットワークの 1 PE ルータだけ取りはずされた IOSバージョン コードを実行しても、リモート PE ルータに接続されるシステムから来るパケットに脆弱です。 このような場合、回避策は正常にこの脆弱性を軽減するためにすべての PE ルータで展開される必要があります。

mdt データ <group> <mask> か **mdt データ <group> <mask> しきい値 <n> リスト <acl>** コマンドはこの脆弱性を軽減しません。

UDP ポート 3232 へのフィルタリングパケット

MDT データ 加入 メッセージは UDP ポート 3232 に送信 されます。 access-list の作成 PE ルータの VRF インターフェイスの宛先 UDP 加えポート 3232 および加えることをそれをフィルタリングするこの脆弱性を軽減します。 そのようなこのように access-list な:

```
Router>show version
    Cisco IOS Software, 7200 Software (C7200-IK9S-M), Version 12.3(14)T1, RELEASE SOFTWARE (fc1)
    Technical Support: http://www.cisco.com/techsupport
    Copyright (c) 1986-2005 by Cisco Systems, Inc.
    Compiled Thu 31-Mar-05 08:04 by yiyan
```

この access-list がまた UDP ポート 3232 に向かう正当なトラフィックをフィルタリングできることに注目して下さい。 このような場合、access-list は個々の BGPピア IP アドレスの提供によって特定であるために修正することができます。 続くこれはセクションで説明されます。

VRF インターフェイスの BGPピア IP アドレスのフィルタリング

正常にこの脆弱性を不正利用するために、攻撃者は既存の iBGP 同位の 1 の IP アドレスからのパケットのスプーフィングによって MDT データ 加入 メッセージを送信 する必要があります。 MDT データ 加入 メッセージが PE ルータの間だけで使用されるので、CE デバイスからのパケットは安全にフィルタ処理されたである場合もあります。

access-list の作成 PE ルータの VRF インターフェイスで送信元アドレスおよびそれを適用することがこの脆弱性を軽減すると同時に iBGP ピア IP アドレスをフィルタリングする。 すべての iBGP ピア IP アドレスをフィルタリングする access-list 必要。 そのようなこの例のように access-list 見え:

```
Router>show version
    Cisco IOS Software, 7200 Software (C7200-IK9S-M), Version 12.3(14)T1, RELEASE SOFTWARE (fc1)
    Technical Support: http://www.cisco.com/techsupport
    Copyright (c) 1986-2005 by Cisco Systems, Inc.
    Compiled Thu 31-Mar-05 08:04 by yiyan
```

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:

326-mvpn

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	12.0(32)S9 12.0(33)S	
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	脆弱性あり; contact TAC	
12.0SY	12.0(32)SY4	
12.0SZ	12.0(30)SZ4	
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**
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)BC 1
12.2BW	脆弱性なし	
12.2BY	脆弱性なし	
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)BC 1
12.2CY	脆弱性なし	
12.2CZ	脆弱性あり; contact TAC	
12.2DA	脆弱性なし	
12.2DD	脆弱性なし	
12.2DX	脆弱性なし	
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(37)EX	12.2(40)EX 1
12.2EY	12.2(37)EY	
12.2EZ	脆弱性あり; first fixed in	

	12.2SEE	
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(44)SE1
12.2IXA	脆弱性あり; first fixed in 12.2IXD	
12.2IXB	脆弱性あり; first fixed in 12.2IXD	
12.2IXC	脆弱性あり; first fixed in 12.2IXD	
12.2IXD	12.2(18)IXD1	
12.2IXE	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	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	脆弱性なし	
12.2SEG	12.2(25)SEG3	12.2(25)SEG4
12.2SG	12.2(25)SG2 12.2(31)SG2 12.2(37)SG1	12.2(44)SG

	12.2(40)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	12.2(29)SM2	
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	12.2(25)SW11	
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)SXF10 12.2(18)SXF10a 12.2(18)SXF12a	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	脆弱性なし	
12.2UZ	脆弱性あり; first fixed in	12.2(31)SB

	12.2SB; 31-MAR-2008 で利用可能	11
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	12.2(33)XN1	12.3(26)
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	脆弱性なし	
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	脆弱性なし	
12.2YP	脆弱性なし	
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	脆弱性なし	
12.2YX	脆弱性あり; first fixed in 12.4	12.4(18a)
12.2YY	脆弱性なし	
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	脆弱性なし	
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	12.2(18)ZY1	12.2(18)ZY2
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(21b) 12.3(22a) 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	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	Release prior to 12.3(8)JK1 are vulnerable， releases 12.3(8)JK1 and later are not vulnerable;	12.3(8)JK1
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(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)XE5	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)XI10a	
12.3XJ	脆弱性あり; first fixed in 12.3YX	12.3(14)YX 11 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)YX 11 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)YX 11 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)YS2	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)YX9	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(12b) 12.4(13c) 12.4(16) 12.4(3h) 12.4(5c) 12.4(7f) 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	12.4(11)MD1	12.4(15)MD; 09-MAY-08 で利用可能
12.4MR	12.4(12)MR2	12.4(16)MR2
12.4SW	12.4(11)SW3	12.4(15)SW
12.4T	12.4(11)T3 12.4(15)T 12.4(2)T6 12.4(4)T8 12.4(6)T8 12.4(9)T4	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)XD8	12.4(4)XD10
12.4XE	12.4(6)XE2	12.4(15)T4
12.4XF	脆弱性あり; first fixed in 12.4T	12.4(15)T4
12.4XG	12.4(9)XG2	12.4(9)XG2
12.4XJ	12.4(11)XJ4	12.4(15)T4
12.4XK	脆弱性あり; first fixed in 12.4T	12.4(15)T4
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。

この脆弱性はトマス Morin によって Cisco に報告されました。

出典

URL

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

改訂履歴

リビジョン 1.3	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 1.2	2008-April-22	CVSSCSCSI01470 の更新済 URL。
リビジョン 1.1	2008-March-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。
リビジョン	2008-March-26	初回公開リリース

1.0		

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。