Cisco IOSマルチキャストバーチャルプライベートネットワーク(MVPN)のデータリーク

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

シスコのMulticast Virtual Private Network(MVPN)の実装における脆弱性は、悪意のあるユーザがコアルータ上で追加のマルチキャストステートを作成したり、特別に巧妙に細工されたメッセージを送信して他のMultiprotocol Label Switching(MPLS)ベースのVirtual Private Network（VPN；バーチャルプライベートネットワーク）からマルチキャストトラフィックを受信したりすることを可能にする可能性がある不正利用の対象となります。

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ています。こ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、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-mvpn で公開されています。

注：2008年3月26日公開のSecurity Advisoryは5件あります。これらのアドバイザリはすべてCisco IOSに影響します。各アドバイザリには、このアドバイザリで説明されている脆弱性を修正したリリースが記載されています。また、この5つのアドバイザリで説明されている脆弱性を修正したリリースの詳細についても記載されています。

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のDoS脆弱性
  https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-pptp
- Cisco IOSにおける複数のDLSwサービス拒否の脆弱性
  https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-

20080326-dlsw

- IPv4/IPv6デュアルスタックルータに関するCisco IOSユーザデータグラムプロトコル(UDP)配信の問題
  https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-IPv4IPv6
- OSPF、MPLS VPN、Supervisor 32、Supervisor 720、またはRoute Switch Processor 720を使用するCisco IOSの脆弱性
  https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-queue
- Cisco IOSマルチキャストバーチャルプライベートネットワーク(MVPN)のデータリーク
  https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-mvpn

該当製品

脆弱性のある製品

Cisco IOSが稼働し、MVPNが設定されているデバイスが影響を受けます。

MVPN用に設定されたIOSデバイスには、実行コンフィギュレーションの例に次のような行があります。

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

Cisco IOS製品で稼働しているソフトウェアを判別するには、デバイスにログインしてshow versionコマンドを発行し、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」として識別されます。 出力の次の行では、カッコ内にイメージ名が表示され、その後に「Version」とCisco IOSリリース名が続きます。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、IOSイメージが稼働しているデバイスからの出力結果を示しています。

```
<#root>

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リリースの命名に関する詳細については、
http://www.cisco.com/warp/public/620/1.htmlを参照してください。

脆弱性を含んでいないことが確認された製品

IOS XRソフトウェアを含む他のシスコ製品において、この脆弱性の影響を受けるものは現在確認されていません。

詳細

MVPNアーキテクチャでは、サービスプロバイダーがMPLS VPNでマルチキャストトラフィックをサポートするために役立つ追加のプロトコルと手順が導入されています。MVPNを使用すると、プロバイダーのMPLS VPNバックボーン上でIPマルチキャストトラフィックを透過的に転送でき、サービスプロバイダーはMPLS VPNカスタマーにマルチキャストサービスを提供できます。

MVPNの実装には脆弱性が存在します。この脆弱性により、攻撃者は特別に巧妙に細工されたマルチキャスト配布ツリー(MDT)データ結合メッセージを送信でき、コアルータで余分なマルチキャスト状態が作成される可能性があります。MDTデータ加入メッセージは、ユニキャストまたはマルチキャストで送信できます。この脆弱性により、異なるMPLS VPNからのマルチキャストトラフィックの漏洩が可能になる場合もあります。同じプロバイダーエッジ(PE)ルータに接続されていないVPNからマルチキャストトラフィックを受信することができます。攻撃者がこの脆弱性を不正利用するには、リモートPEルータのBorder Gateway Protocol(BGP)ピアリングIPアドレスと、他のMPLS VPNで使用されているマルチキャストグループのアドレスを知っているか、推測する必要があります。

この脆弱性は、Cisco Bug ID CSCsi01470（登録ユーザ専用）として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2008-1156が割り当てられています。

回避策

この脆弱性の回避策は、PEデバイス上のMDTデータ結合パケットのフィルタリングで構成されます。

回避策は、すべてのPEルータのすべてのVirtual Routing and Forwarding(VRF)インターフェイスに適用する必要があります。そうしないと、攻撃者はリモートPEルータをターゲットとすることができ、引き続きこの脆弱性を不正利用する可能性があります。

ネットワーク内の1台のPEルータのみが修正前のバージョンのIOSコードを実行している場合でも、リモートPEルータに接続されているシステムからのパケットに対して脆弱です。このような場合、この脆弱性を軽減するには、すべてのPEルータに回避策を導入する必要があります。

mdt data <group> <mask>コマンドまたはmdt data <group> <mask> threshold <n> list <acl>コマンドでは、この脆弱性は緩和されません。

UDPポート3232へのパケットのフィルタリング

MDTデータ加入メッセージはUDPポート3232に送信されます。宛先UDPポート3232をフィルタリングするアクセスリストを作成し、PEルータのVRFインターフェイスに適用することで、この脆弱性を緩和できます。このようなアクセスリストは次のようになります。

```
access-list 100 deny udp any any eq 3232
access-list 100 permit ip any any

interface Serial 0/0
  ip vrf forwarding <vpn-1>
  ...
  ip access-group 100 in
```

このアクセスリストでは、UDPポート3232宛ての正当なトラフィックもフィルタリングできることに注意してください。このような場合、個々のBGPピアのIPアドレスを指定することで、アクセスリストをより具体的に変更できます。これについては、次のセクションで説明します。

VRFインターフェイスでのBGPピアのIPアドレスのフィルタリング

この脆弱性を不正利用するには、攻撃者は既存のiBGPピアの1つのIPアドレスからパケットをスプーフィングすることによってMDT Data Joinメッセージを送信する必要があります。MDTデータ結合メッセージはPEルータ間でのみ使用されるため、CEデバイスからのパケットは安全にフィルタリングできます。

iBGPピアのIPアドレスを送信元アドレスとしてフィルタリングするアクセスリストを作成し、PEルータのVRFインターフェイスに適用することで、この脆弱性を緩和できます。アクセスリストは、すべてのiBGPピアのIPアドレスをフィルタリングする必要があります。このようなアクセスリストは次の例のようになります。

```
access-list 100 deny udp host <ibgp-peer-1> any eq 3232
access-list 100 deny udp host <ibgp-peer-2> any eq 3232
...
access-list 100 deny udp host <ibgp-peer-n> any eq 3232
access-list 100 permit ip any any

interface Serial 0/0
  ip vrf forwarding <vpn-1>
  ...
  ip access-group 100 in
```

ネットワーク内のCiscoデバイスに展開できる追加の緩和テクニックについては、このアドバイザリに関連するCisco適用対応策速報を参照してください。

https://sec.cloudapps.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20080326-mvpn

修正済みソフトウェア

アップグレードを検討する場合は、http://www.cisco.com/go/psirt と後続のアドバイザリも参照して、問題の解決状況と完全なアップグレード ソリューションを確認してください。

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、TACに連絡	
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(最初の修正は12.4)	12.4(18a)
12.2BC	脆弱性あり(最初の修正は12.3BC)	12.3(23)BC1
12.2BW	脆弱性なし	
12.2BY	脆弱性なし	
12.2BZ	脆弱性あり(最初の修正は12.3XI)	
12.2CX	脆弱性あり(最初の修正は12.3BC)	12.3(23)BC1

12.2CY	脆弱性なし	
12.2CZ	脆弱性あり。TACに連絡	
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(最初の修正は12.2SG)	12.2(25)EWA13 12.2(31)SGA5 12.2(44)SG
12.2EW	脆弱性あり(最初の修正は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)EX1
12.2EY	12.2(37)EY	
12.2EZ	脆弱性あり(最初の修正は12.2SEE)	

12.2FX	脆弱性なし	
12.2FY	脆弱性なし	
12.2FZ	脆弱性あり(最初の修正は12.2SE)	12.2(44)SE1
12.2IXA	脆弱性あり(最初の修正は12.2IXD)	
12.2IXB	脆弱性あり(最初の修正は12.2IXD)	
12.2IXC	脆弱性あり(最初の修正は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)S15

	12.2(25)S13	
12.2SB	12.2(28)SB7 12.2(31)SB5 12.2(33)SB（2008年3月31日に入手可能）	12.2(31)SB11
12.2SBC	脆弱性あり。最初の修正は12.2SB。2008年3月31日に入手可能	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(最初の修正は12.2SEE)	
12.2SEB	脆弱性あり(最初の修正は12.2SEE)	
12.2SEC	脆弱性あり(最初の修正は12.2SEE)	
12.2SED	脆弱性あり(最初の修正は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(40)SG	12.2(44)SG
12.2SGA	12.2(31)SGA2 12.2(31)SGA3 12.2(31)SGA6（2008年4月7日に入手可能）	12.2(31)SGA5
12.2SL	脆弱性なし	
12.2SM	12.2(29)SM2	
12.2SO	脆弱性あり。 12.2SVAの任意のリリースに移行	12.2(29)SVD
12.2SRA	12.2(33)SRA4	12.2(33)SRA7
12.2SRB	12.2(33)SRB1	12.2(33)SRB3（2008年4月14日に入手可能）
12.2SRC	脆弱性なし	
12.2SU	脆弱性あり(最初の修正は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(最初の修正は12.2SXF)	12.2(18)SXF13
12.2SXA	脆弱性あり(最初の修正は12.2SXF)	12.2(18)SXF13
12.2SXB	脆弱性あり(最初の修正は12.2SXF)	12.2(18)SXF13
12.2SXD	脆弱性あり(最初の修正は12.2SXF)	12.2(18)SXF13
12.2SXE	脆弱性あり(最初の修正は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(最初の修正は12.2SXF)	12.2(18)SXF13
12.2SZ	脆弱性あり(最初の修正は12.2S)	12.2(25)S15 12.2(31)SB11 12.2(33)SRC
12.2T	脆弱性あり。最初の修正は12.3	12.3(26)
12.2TPC	脆弱性なし	
12.2UZ	脆弱性あり。最初の修正は12.2SB。2008年3月31日に入手可能	12.2(31)SB11
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。最初の修正は12.3	12.3(26)
12.2YJ	脆弱性あり。最初の修正は12.3	12.3(26)
12.2YK	脆弱性なし	
12.2YL	脆弱性あり(最初の修正は12.4)	12.4(18a)
12.2YM	脆弱性あり(最初の修正は12.4)	12.4(18a)
12.2YN	脆弱性あり(最初の修正は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(最初の修正は12.4)	12.4(18a)
12.2YR	脆弱性あり(最初の修正は12.4)	12.4(18a)
12.2YS	脆弱性なし	
12.2YT	脆弱性あり。最初の修正は12.3	12.3(26)
12.2YU	脆弱性あり(最初の修正は12.4)	12.4(18a)
12.2YV	脆弱性あり(最初の修正は12.4)	12.4(18a)
12.2YW	脆弱性なし	
12.2YX	脆弱性あり(最初の修正は12.4)	12.4(18a)
12.2YY	脆弱性なし	
12.2YZ	脆弱性あり(最初の修正は12.2S)	12.2(25)S15 12.2(31)SB11 12.2(33)SRC
12.2ZA	脆弱性あり(最初の修正	12.2(18)SXF13

	は12.2SXF)	
12.2ZB	脆弱性なし	
12.2ZC	脆弱性あり(最初の修正は12.4)	12.4(18a)
12.2ZD	脆弱性あり。TACに連絡	
12.2ZE	脆弱性あり。最初の修正は12.3	12.3(26)
12.2ZF	脆弱性あり(最初の修正は12.4)	12.4(18a)
12.2ZG	脆弱性あり(最初の修正は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(最初の修正は12.4)	12.4(18a)
12.2ZL	脆弱性あり(最初の修正は12.4)	12.4(15)T4 12.4(18a)
12.2ZP	脆弱性あり(最初の修正は12.4)	12.4(18a)
12.2ZU	脆弱性あり。	12.2(33)SXH2

	12.2SXHの任意のリリースに移行	
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(最初の修正は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(最初の修正は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	12.3(8)JK1より前のリリースには脆弱性があり、12.3(8)JK1以降のリリースには脆弱性はありません。	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(最初の修正は12.4)	12.4(18a)
12.3TPC	12.3(4)TPC11b	
12.3VA	脆弱性あり。TACに連絡	
12.3XA	12.3(2)XA6	12.3(2)XA7（2008年3月31日に入手可能）
12.3XB	脆弱性あり(最初の修正は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(最初の修正は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(最初の修正は12.4)	12.4(18a)
12.3XG	脆弱性あり(最初の修正は12.3YG)	12.4(15)T4 12.4(18a)
12.3XH	脆弱性あり(最初の修正は12.4)	12.4(18a)
12.3XI	12.3(7)XI10a	
12.3XJ	脆弱性あり(最初の修正は12.3YX)	12.3(14)YX11 12.4(15)T4
12.3XK	脆弱性あり(最初の修正は12.4)	12.4(18a)
12.3XQ	脆弱性あり(最初の修正は12.4)	12.4(18a)
12.3XR	12.3(7)XR7	12.3(7)XR8（2008年3月31日に入手可能）

12.3XS	脆弱性あり(最初の修正は12.4)	12.4(18a)
12.3XU	脆弱性あり(最初の修正は12.4T)	12.4(15)T4
12.3XW	脆弱性あり(最初の修正は12.3YX)	12.3(14)YX11 12.4(15)T4
12.3XY	脆弱性あり(最初の修正は12.4)	12.4(18a)
12.3YA	脆弱性あり(最初の修正は12.4)	12.4(15)T4 12.4(18a)
12.3YD	脆弱性あり(最初の修正は12.4T)	12.4(15)T4
12.3YF	脆弱性あり(最初の修正は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(最初の修正は12.4T)	12.4(15)T4
12.3YI	脆弱性あり(最初の修正は12.4T)	12.4(15)T4
12.3YJ	脆弱性あり(最初の修正は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(最初の修正は12.4T)	12.4(15)T4
12.3YS	12.3(11)YS2	12.4(15)T4
12.3YT	脆弱性あり(最初の修正は12.4T)	12.4(15)T4
12.3YU	脆弱性あり(最初の修正は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(18a)

	12.4(7f) 12.4(8d)	
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（2008年5月9日に入手可能）
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(最初の修正は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(最初の修正は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(最初の修正は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	

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例やその公表は確認しておりません。

この脆弱性は、Thomas Morin氏によってシスコに報告されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-mvpn

改訂履歴

リビジョン 1.3	2008年6月27日	概要を更新して、リンクと文言を削除しました。
リビジョン 1.2	2008年4月22日	CVSSCSCsi01470のURLを更新。
リビ	2008年3月	アドバイザリID cisco-sa-20080326-IPv4IPv6（IPv4IPv6デュアルスタックル

ジョン1.1	29日	ータに関する3月26日のアドバイザリ）に関する新しい情報が追加されたため、12.0S、12.0SY、12.0SX、および12.0SZのソフトウェアテーブルを更新。
リビジョン1.0	2008年3月26日	初回公開リリース

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。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。