インフラストラクチャ サービス拒否の脆弱性を転送する Cisco IOS MPLS

High

アドバイザリーID : cisco-sa-20080924-mfi

初公開日 : 2008-09-24 16:00

バージョン 1.1 : Final

CVSSスコア : 7.8

回避策 : No Workarounds available

Cisco バグ ID : CSCsk93241

CVE-2008-3804

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

インフラストラクチャ（MFI）を転送する Cisco IOSソフトウェア Multi Protocol Label Switching（MPLS）は特別に 巧妙に細工されたパケットからのサービス拒絶（DoS）攻撃に脆弱です。 MFI だけこの脆弱性から影響を受けます。 MFI と取替えられるより古いラベル転送情報ベース（LFIB）実装は影響を受けていません。

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。

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

該当製品

（MPLS のために設定される場合 Cisco IOSソフトウェア モジュール性をサポートするを含むそれら Cisco IOSソフトウェア）およびサポート MFI を実行するデバイスは影響を受けている。

脆弱性のある製品

Cisco IOSソフトウェアおよびサポート MFI を実行するデバイスに **show subsys コマンド**の出力の **mfi_ios が**あります。 次の例は MFI をサポートするデバイスからの出力を示したものです:

```
Router#show subsys name mfi_ios
             Class         Version
mfi_ios      Protocol    1.000.001
Router#
```

次の例は MPLS のために設定されるデバイスからの出力を示したものです:

```
Router#show mpls interface
Interface      IP           Tunnel  BGP Static Operational
Ethernet0/0    Yes (ldp)    No      No  No     Yes
Router#
```

デバイスに Cisco製品、ログインで動作するソフトウェアを判別し、システムバナーを表示する " show version " コマンドを発行するため。 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 IOSリリース名の間で表示する。 他の Ciscoデバイスに" show version " コマンドがありませんまたはために別の出力を与えて下さい。

次の例は Cisco IOS Release 12.4(11)T2 を実行している Cisco製品を指定したものです:

```
Router#show version
Cisco IOS Software,7200 Software (C7200-ADVSECURITYK9-M), Version 12.4(11)T2, RELEASE SOFTWARE
(fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Tue 01-May-07 04:19 by prod_rel_team

 <output truncated>
```

Cisco IOSリリース命名規則のその他の情報は「白書と資格を与えられる文書で見つけることができます: http://www.cisco.com/warp/public/620/1.html で利用可能である Cisco IOSレファレンスガイド」、

脆弱性を含んでいないことが確認された製品

MFI が含まれていない実行するデバイス Cisco IOS ソフトウェア バージョンは脆弱ではないです。

MPLS のために設定されないデバイスは脆弱ではないです。

Cisco IOS XR ソフトウェアを実行しているデバイスは脆弱ではないです。

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

Cisco IOSソフトウェアの新しいバージョンではスケーラビリティおよびパフォーマンスを改善するために、新しいパケット転送 インフラストラクチャはもたらされました。 MFI と呼ばれるこのフォワーディング インフラストラクチャはユーザに対して透過的です。 MFI は転送のために使用される MPLS データ構造を管理し、より古い実装を、ラベル転送情報ベース （LFIB）取り替えます。 Cisco IOS MFI 実装はソフトウェアパスで処理されるソフトウェアパスで処理される中継パケットを含む特別に 巧妙に細工されたパケットからの DoS攻撃に脆弱です。 そのようなパケットはローカルセグメントから MPLS のためにまたは MPLS のために設定されるトンネルインターフェイスによって設定されるインターフェイスに送信することができます。 MPLS ネットワークのリモート システムを目標とするために、攻撃者は MPLS使用可能 な インターフェイスを通して MPLS ネットワークにアクセスできる必要があります。 MPLS パケットは MPLS のために設定されないインターフェイスで廃棄されます。

MFI をサポートするデバイスに **show subsys コマンド**の出力の **mfi_ios が**あります。 MPLS のために有効に なる インターフェイスは**提示 MPLS interface コマンド**によって参照される場合があります。

MFI に関する詳細は次のリンクで見つけることができます:

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_lsc_removed.html

この脆弱性 Cisco バグ ID **CSCsk93241** （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-2008-3804 は割り当てられました。

回避策

MPLS は他の MPLS使用可能 な デバイスによって共有される論理インターフェイスおよび物理的で普通有効に なります。 それは MPLS が必要ではないインターフェイスで潜在的なアタックが開始することができるかどれからディセーブルにすることができ。 この操作はこの脆弱性の公開の制限を助けるかもしれません。

攻撃が開始することができるインターフェイスの MPLS をディセーブルにすることはできない場合この脆弱性を軽減する回避策がありません。

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**
該当する 12.0 ベースのリリースはありません。		
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	12.2(44)EY; 16-DEC-08 で利用可能	
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	12.2(22)S 以前のリリースは脆弱ではないです。 12.2(30)S 前のリリース 12.2(22)S およびそれ以降は脆弱であり、 リリース 12.2(30)S およびそれ以降は脆弱ではないです	12.2(33)SB2; 26-SEP-08 で利用可能
12.2SB	12.2(31)SB12 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	12.2(33)SCA1	12.2(33)SCA1
12.2SE	12.2(44)SE3; 30-SEP-08 で利用可能 12.2(46)SE	12.2(46)SE
12.2SEA	脆弱性なし	
12.2SEB	脆弱性なし	
12.2SEC	脆弱性なし	
12.2SED	脆弱性あり; first fixed in 12.2SE	12.2(46)SE
12.2SEE	脆弱性あり; first fixed in 12.2SE	12.2(46)SE
12.2SEF	脆弱性なし	
12.2SEG	注： Release prior to 12.2(25)SEG4 are vulnerable，releases 12.2(25)SEG4 and later are not vulnerable;	12.2(25)SEG6
12.2SG	12.2(50)SG; 24-NOV-08 で利用可能	12.2(46)SG1
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	脆弱性あり; first fixed in 12.2SRB	12.2(33)SRB4 12.2(33)SRC2
12.2SRB	12.2(33)SRB4	12.2(33)SRB4
12.2SRC	12.2(33)SRC1	12.2(33)SRC2
12.2SU	脆弱性なし	
12.2SV	脆弱性あり; contact TAC	
12.2SVA	脆弱性あり; contact TAC	
12.2SVC	脆弱性あり; contact TAC	
12.2SVD	脆弱性あり; contact TAC	
12.2SW	注： Release prior to 12.2(25)SW4 are vulnerable，releases 12.2(25)SW4 and later are not vulnerable;	12.2(25)SW12
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	12.2(33)SXH3	12.2(33)SXH3
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	脆弱性あり; first fixed in 12.2SB	12.2(33)SB2; 26-SEP-08 で利用可能 12.2(33)SRC2 12.2(33)XNA2
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**
該当する 12.3 ベースのリリースはありません。		
Affected 12.4-	First Fixed Release (修正された最初のリリース)	**推奨リリース**

Based Releases		
12.4	脆弱性なし	
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	12.4(15)XQ1	12.4(15)XQ1
12.4XR	脆弱性あり; migrate to any release in 12.4T	12.4(15)T7
12.4XT	脆弱性なし	
12.4XV	脆弱性なし	
12.4XW	脆弱性なし	
12.4XY	12.4(15)XY4	12.4(15)XY4
12.4XZ	12.4(15)XZ1	12.4(15)XZ2
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。

この脆弱性はシスコ内部で発見されました。

出典

URL

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

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