Cisco IOSソフトウェア H.323 サービス拒否の脆弱性

High	**アドバイザリーID :** cisco-sa-20090923-h323 **初公開日 :** 2009-09-23 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 :** CSCsz38104	CVE-2009-2866

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 IOSÂ® ソフトウェアの H.323 実装はリロードするために Cisco IOSソフトウェアを実行しているデバイスを引き起こすのにリモートで不正利用することができる脆弱性が含まれています。

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。Cisco IOSソフトウェアを実行しているデバイスが VOIPサービスのための H.323 を実行する必要はない場合 H.323 をディセーブルにすることから離れて脆弱性を軽減する回避策がありません。

このアドバイザリは 923-h323 で掲示されます。

注: 2009 年 9 月 23 日の IOS アドバイザリ バンドル公開には 11 件の Security Advisory が含まれています。 10 件のアドバイザリは Cisco IOS ソフトウェアの脆弱性に対処するもので、 1 件は Cisco Unified Communications Manager の脆弱性に対処するものです。 各アドバイザリには、そのアドバイザリで詳述された脆弱性を解決するリリースを記載しています。

"Cisco Event Response: Semiannual Cisco IOS Software Advisory Bundled Publication" の個々の公開リンクは次のリンク内に掲載されています:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep09.html

該当製品

脆弱性のある製品

H.323 メッセージを処理するために設定される影響を受けた Cisco IOS ソフトウェア バージョンを実行している Ciscoデバイスはこの脆弱性から影響を受けます。 H.323 はデフォルトで有効に なりません。

Cisco IOSソフトウェア デバイスを判別することは H.323 サービスを使用します **show process CPU を**経営しています | 次の例に示すように **323** コマンドを、**含んで下さい**:

```
Router#show process cpu | include 323
 249       16000           3       5333  0.00%  0.00%  0.00%    0 CCH323_CT
 250           0           1          0  0.00%  0.00%  0.00%    0 CCH323_DNS
Router#
```

注: H.323 リスニングポート TCP 1720 だけ影響を受けています。

シスコ製品上で動作している Cisco IOS ソフトウェア リリースについては、管理者が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 バナーを表示することで判別できます。 "Internetwork Operating System Software"、"Cisco IOS Software" あるいはこれらに類似するシステム バナーによってデバイスで Cisco IOS ソフトウェアが稼働していることを確認できます。 その後ろにイメージ名が括弧の間に表示され、続いて "Version" と Cisco IOS ソフトウエア リリース名が表示されます。 他のシスコ デバイスでは、**show version** コマンドが存在しなかったり、別の出力が表示されたりします。

以下の例は、Cisco 製品にて、IOSリリース 12.3(26) が稼動し、そのイメージ名が C2500-IS-L であることを示しています:

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih

!--- output truncated
```

次の例は C1841-ADVENTERPRISEK9-M のインストール済みイメージ名前と Cisco IOS ソフトウェア リリース 12.4(20)T 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, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE
SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

!--- output truncated
```

Cisco IOS ソフトウエアのリリース命名規則の追加情報は以下のリンクの "White Paper: Cisco IOS Reference Guide" で確認できます: 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

Cisco IOS XE および 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

H.323 はパケット ベース（IP）ネットワーク上のリアルタイム マルチメディア通信および会議のための ITU 規格です。 H.323 規格のサブセットは H.225.0、IP ネットワーク上のコール通知プロトコルおよびメディア ストリーム パケット化に使用する規格です。

Cisco IOSソフトウェアの H.323 実装は脆弱性が含まれています。 攻撃者は Cisco IOSソフトウェアを実行している影響を受けたデバイスへ H.323 によって細工 される パケットを送信 することによってこの脆弱性をリモートで不正利用できます。 TCP 3 ウェイ ハンドシェイクは必要この脆弱性を不正利用するためにです。

この脆弱性 Cisco バグ ID **CSCsz38104**（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-2009-2866 は割り当てられました。

回避策

Cisco IOSデバイスが VOIPサービスのための H.323 を実行する必要はない場合 H.323 をディセーブルにすることから離れて脆弱性を軽減する回避策がありません。 H.323 を実行する必要がある影響を受けたデバイスは脆弱で、そこにそれらを保護するのに使用できる特定のコンフィギュレーションではないです。 戦略的な場所の置くファイアウォール H.323 トラフィックを受け入れるべきではないインターフェイスのアクセス リストを追加することはアップグレードが実行されたことができるまで公開を大幅に減らすかもしれ。

Cisco は助けるようにソリューション リファレンス ネットワーク デザイン（SRND）ガイドを提供します http://www.cisco.com/go/srnd 音声セキュリティ上の推奨事項で見つけることができるネットワーキング ソリューションを設計・展開することは http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/6x/security.html の Cisco Unified Communications SRND によって基づく Unified Communications Manager 6.x で、on Cisco カバーされます。

どこでもからの H.323 マネジメントトラフィックしかし許可されたネットワークをブロックするアクセス リストの例は下記にあります。 この例では、許可されたネットワークは 172.16.0.0/16 です。

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE SOFTWARE
(fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

!--- output truncated
```

また、次の例に示すように**音声 サービス VOIPモード**の下で**コール サービス停止によって強制される**コマンドを、使用できます:

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE SOFTWARE
(fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team

!--- output truncated
```

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軽減はドキュメントガイド「Cisco で利用できます加えました軽減情報を: 」次の位置で利用可能である Cisco Unified Communications Manager および Cisco IOSソフトウェアのサービス拒否の脆弱性の識別し、軽減不正利用、: http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20090923-voice。

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。 「推奨されるリリース」カラムはリリースを示しますこのアドバイザリの時に送達された脆弱性のための修正がある。 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 基づいたリリースがありません。		

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 基づいたリリースがありません。		
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 12.2(4)B8 以前のリリースは脆弱ではないです。	12.4(25b) 12.4(23b)
12.2BC	脆弱性なし	
12.2BW	脆弱性なし	
12.2BX	脆弱性あり; first fixed in 12.4 12.2(15)BX 以前のリリースは脆弱ではないです。	12.4(25b) 12.4(23b)
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	脆弱性あり; 12.2SB への移行する	12.2(33)SB7
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	
12.2IRA	脆弱性なし	
12.2IRB	脆弱性なし	
12.2IRC	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	
12.2IXH	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)MC1 以前のリリースは脆弱ではないです。 リリース 12.2(15)MC2b およびそれ以降は脆弱ではないです; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2S	脆弱性なし	
12.2SB	脆弱性なし	
12.2SBC	脆弱性なし	
12.2SCA	脆弱性なし	
12.2SCB	脆弱性なし	
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	
12.2SQ	脆弱性なし	
12.2SRA	脆弱性なし	
12.2SRB	脆弱性なし	
12.2SR	脆弱性なし	

C		
12.2SRD	脆弱性なし	
12.2STE	脆弱性なし	
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	
12.2SVE	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	
12.2SXI	脆弱性なし	
12.2SY	脆弱性なし	
12.2SZ	脆弱性なし	
12.2T	脆弱性あり; first fixed in 12.4 12.2(8)T10 以前のリリースは脆弱ではないです。	12.4(25b) 12.4(23b)
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	
12.2XNA	脆弱性なし	
12.2XNB	脆弱性なし	
12.2XNC	脆弱性なし	
12.2XND	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	脆弱性あり; このアドバイザリの修正済みソフトウェア取得のセクションの手順ごとのサポート 組織に連絡して下さい	
12.2YJ	脆弱性あり; このアドバイザリの修正済みソフトウェア取得のセクションの手順ごとのサポート 組織に連絡して下さい	
12.2YK	脆弱性なし	
12.2YL	脆弱性あり; このアドバイザリの修正済みソフトウェア取得のセクションの手順ごとのサポート 組織に連絡して下さい	
12.2YM	脆弱性あり; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2YN	脆弱性あり; このアドバイザリの修正済みソフトウェア取得のセクションの手順ごとのサポート 組織に連絡して下さい	
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	脆弱性あり; このアドバイザリの修正済みソフトウェア取得のセクションの手順ごとのサポート 組織に連絡して下さい	
12.2YU	脆弱性あり; このアドバイザリの修正済みソフトウェア取得のセクションの手順ごとのサポート 組織に連絡して下さい	
12.2YV	12.2(11)YV1 以前のリリースは脆弱、リリース 12.2(11)YV1 およびそれ以降ではないです脆弱です	
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	脆弱性あり; このアドバイザリの修正済みソフトウェア取得のセクションの手順ごとのサポート 組織に連絡して下さい	
12.2ZD	脆弱性あり; このアドバイザリの修正済みソフトウェア取得のセクションの手順ごとのサポート 組織に連絡して下さい	
12.2ZE	脆弱性あり; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2ZF	脆弱性あり; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2ZG	脆弱性なし	
12.2ZH	脆弱性あり; first fixed in 12.4	12.4(25b) 12.4(23b)
12.2ZJ	脆弱性あり; このアドバイザリの修正済みソフトウェア取得のセクションの手順ごとのサポート 組織に連絡して下さい	
12.2ZL	脆弱性あり; このアドバイザリの修正済みソフトウェア取得のセクションの手順ごとのサポート 組織に連絡して下さい	
12.2ZP	脆弱性あり; このアドバイザリの修正済みソフトウェア取得のセクションの手順ごとのサポート 組織に連絡して下さい	

12.2ZU	脆弱性なし	
12.2ZX	脆弱性なし	
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	脆弱性あり; first fixed in 12.4	12.4(25b) 12.4(23b)
12.3B	脆弱性あり; first fixed in 12.4	12.4(25b) 12.4(23b)
12.3BC	脆弱性なし	
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	12.3(2)JK3 以前のリリースは脆弱ではないです。 リリース 12.3(8)JK1 およびそれ以降は脆弱ではないです; first fixed in 12.4	12.4(25b) 12.4(23b)
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(25b) 12.4(23b)
12.3TPC	12.3(4)TPC11a 以前のリリースは脆弱ではないです。	
12.3VA	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.3XA	Release prior to 12.3(2)XA7 are vulnerable， releases 12.3(2)XA7 and later are not vulnerable; first fixed in 12.4	12.4(25b) 12.4(23b)
12.3XB	脆弱性あり; このアドバイザリの修正済みソフトウェア取得のセクシ	

	ヨンの手順ごとのサポート 組織に連絡して下さい	
12.3XC	脆弱性あり; first fixed in 12.4	12.4(25b) 12.4(23b)
12.3XD	脆弱性あり; first fixed in 12.4	12.4(25b) 12.4(23b)
12.3XE	脆弱性あり; first fixed in 12.4	12.4(25b) 12.4(23b)
12.3XF	脆弱性あり; このアドバイザリの修正済みソフトウェア取得のセクションの手順ごとのサポート 組織に連絡して下さい	
12.3XG	脆弱性あり; first fixed in 12.4	12.4(25b) 12.4(23b)
12.3XI	注： Release prior to 12.3(7)XI11 are vulnerable， releases 12.3(7)XI11 and later are not vulnerable;	12.2(33)SB7 12.2(31)SB16
12.3XJ	脆弱性あり; migrate to any release in 12.4XN	12.4(15)T10
12.3XK	脆弱性あり; first fixed in 12.4	12.4(25b) 12.4(23b)
12.3XL	脆弱性あり; first fixed in 12.4	12.4(25b) 12.4(23b)
12.3XQ	脆弱性あり; first fixed in 12.4	12.4(25b) 12.4(23b)
12.3XR	脆弱性あり; first fixed in 12.4	12.4(25b) 12.4(23b)
12.3XS	脆弱性なし	
12.3XU	脆弱性あり; first fixed in 12.4T 12.3(8)XU1 以前のリリースは脆弱ではないです。	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.3XW	脆弱性あり; migrate to any release in 12.4XR	12.4(15)XR7 12.4(22)XR
12.3XX	脆弱性あり; first fixed in 12.4	12.4(25b) 12.4(23b)
12.3XY	脆弱性あり; first fixed in 12.4	12.4(25b) 12.4(23b)
12.3XZ	脆弱性あり; first fixed in 12.4	12.4(25b)

		12.4(23b)
12.3YA	脆弱性なし	
12.3YD	脆弱性なし	
12.3YF	脆弱性あり; migrate to any release in 12.4XR	12.4(15)XR7 12.4(22)XR
12.3YG	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009で利用可能
12.3YH	脆弱性なし	
12.3YI	脆弱性なし	
12.3YJ	脆弱性なし	
12.3YK	Release prior to 12.3(11)YK3 are vulnerable， releases 12.3(11)YK3 and later are not vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009で利用可能
12.3YM	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009で利用可能
12.3YQ	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T

		2; 23-OCT-2009 で利用可能
12.3YS	脆弱性あり; first fixed in 12.4T 12.3(11)YS1 以前のリリースは脆弱ではないです。	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.3YT	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.3YU	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.3YX	脆弱性あり; 12.4XR への移行する	12.4(15)XR7 12.4(22)XR
12.3YZ	脆弱性あり; このアドバイザリの修正済みソフトウェア取得のセクションの手順ごとのサポート 組織に連絡して下さい	
12.3ZA	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3

		12.4(24)T2; 23-OCT-2009 で利用可能
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(25b) 12.4(23b)	12.4(25b) 12.4(23b)
12.4GC	脆弱性なし	
12.4JA	脆弱性なし	
12.4JDA	脆弱性なし	
12.4JDC	脆弱性なし	
12.4JDD	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	
12.4JX	脆弱性なし	
12.4MD	脆弱性なし	
12.4MDA	脆弱性なし	
12.4MR	12.4(19)MR3 以前のリリースは脆弱、リリース 12.4(19)MR3 およびそれ以降ではないです脆弱です	
12.4SW	脆弱性なし	
12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T2 12.4(24)T1	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.4XA	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3

		12.4(24)T2; 23-OCT-2009 で利用可能
12.4XB	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.4XC	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.4XD	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.4XE	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.4XF	脆弱性なし	
12.4XG	脆弱性なし	

12.4XJ	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009で利用可能
12.4XK	脆弱性なし	
12.4XL	脆弱性あり; このアドバイザリの修正済みソフトウェア取得のセクションの手順ごとのサポート 組織に連絡して下さい	
12.4XM	脆弱性あり; first fixed in 12.4T 12.4(15)XM 以前のリリースは脆弱ではないです。	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009で利用可能
12.4XN	脆弱性なし	
12.4XP	脆弱性あり; このアドバイザリの修正済みソフトウェア取得のセクションの手順ごとのサポート 組織に連絡して下さい	
12.4XQ	脆弱性なし	
12.4XR	脆弱性なし	
12.4XT	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009で利用可能
12.4XV	脆弱性あり; このアドバイザリの修正済みソフトウェア取得のセクションの手順ごとのサポート 組織に連絡して下さい	
12.4XW	脆弱性あり; first fixed in 12.4T	12.4(15)T

		10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.4XY	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.4XZ	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.4YA	脆弱性あり; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; 23-OCT-2009 で利用可能
12.4YB	12.4(22)YB4	12.4(22)YB4
12.4YD	脆弱性なし	
12.4YE	脆弱性なし	

注: Cisco IOS XE ソフトウェアか Cisco IOSソフトウェア モジュール性リリースはこの脆弱性から影響を受けしません。

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-20090923-h323

改訂履歴

リビジョン 1.0	2009-September-23	初版リリース

利用規約