多重 Cisco IOS Session Initiation Protocol（SIP）サービス拒否の脆弱性

High

アドバイザリーID： cisco-sa-20080924-sip

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： CSCse56800 CSCsg91306 CSCsk42759

CVE-2008-3799
CVE-2008-3800
CVE-2008-3801
CVE-2008-3802

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

多重 脆弱点はメモリリークを引き起こすか、または IOSデバイスのリロード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 Cisco IOS のセッション開始プロトコル（SIP）実装にあります。

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。 ソフトウェア バージョン および 修正 セクションにリストされている固定 Cisco IOSソフトウェアはこのアドバイザリで当たるすべての脆弱性のための修正が含まれています。

管理者は Cisco IOSデバイスが Voice over IP サービスを提供するように要求しない場合、利用可能 な 回避策が脆弱性の何れかの効果をプロトコルをディセーブルにすることから離れて軽減するか、またはそれ自身を特色にするためにありません。

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

有効に なる SIP 音声 サービスがあるこれらの脆弱性は実行するデバイス Cisco IOS だけに影響を与えます。

脆弱性のある製品

影響を受けた Cisco IOSバージョンを実行する Ciscoデバイスおよびそれは影響を受けています SIP メッセージを処理するかもしれません。 これらの脆弱性のための唯一の要件は Cisco IOSデバイスが IP （ VoIP ）機能上の構成された音声の一部として SIP メッセージを処理することです (これは NAT およびファイアウォール フィーチャ セットの一部として SIP メッセージの処理に適用しません。 ） Cisco IOS の最近のバージョンは SIP メッセージをデフォルトで処理しませんが、コマンド **dial-peer voice** による「ダイヤル ピア」を作成することは SIP プロセスを開始し、Cisco IOS を SIP メッセージを処理し始めさせます。 影響を受けた設定の例は次の通りです:

```
dial-peer voice <Voice dial-peer tag> voip
 ...
!
```

Cisco IOS のより古いバージョンが Cisco IOS が SIP オペレーションのために設定されないで SIP メッセージを不具合から影響を受けたことに注目して下さい処理しました。 その他の情報バグID **CSCsb25337** （ 登録ユーザのみ ）のための http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070131-sip を on Cisco 参照して下さい。

デバイスが SIP メッセージを処理します**ダイヤルピアコマンド**のために Cisco IOSデバイス 設定を点検することに加えて管理者はまたいくつかの **show コマンドを**使用できます SIP メッセージを処理する、またはかどうか Cisco IOSデバイスがプロセスを実行した確認するデバイス

が SIP ポートで受信すれば。

コマンド **show processes | SIP を** Cisco IOS が SIP メッセージを処理するプロセスを実行しているかどうか判別するのに使用することができます**含んで下さい**。 次の例では、Cisco IOSデバイスが SIP メッセージを処理していることをプロセス **CCSIP_UDP_SOCKET** の存在および **CCSIP_TCP_SOCKET は**示します:

```
Router#show processes | include SIP
 147 Mwe 40F46DF4           12          2    600023468/24000  0 CCSIP_SPI_CONTRO
 148 Mwe 40F21244            0          1       0 5524/6000   0 CCSIP_DNS
 149 Mwe 40F48254            4          1    400023108/24000  0 CCSIP_UDP_SOCKET
 150 Mwe 40F48034            4          1    400023388/24000  0 CCSIP_TCP_SOCKET
```

Cisco IOS の異なるバージョンに Cisco IOSデバイスが SIP メッセージを聞き取っているかどうか確かめるさまざまな方法があります。 **show ip sockets は**、**show udp**、**show tcp 要約すべて**、これらのコマンドすべてがすべての IOS リリースで動作しないが**コントロール・プレーン ホスト 開港**コマンドがこれを判別するのに使用することができることを**示し**。 さまざまなリリースに相当してコマンドのリストを提供するためにそれがこの文書で実用的ではないのでユーザははたらくどれがデバイスのために判別する前述コマンドを試す必要があります。 以下はポート 5060 （ SIP ポート ）で受信するルータを示す 1 コマンドの 1 つの例です:

```
router#show control-plane host open-ports
Active internet connections (servers and established)
Prot        Local Address      Foreign Address                  Service    State
<output removed for brevity>
 tcp               *:5060                   *:0                     SIP   LISTEN
<outoput removed for brevity>
 udp               *:5060                   *:0                     SIP   LISTEN
```

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-ADVSECURITYK9-M), Version 12.4(6)T2, RELEASE SOFTWARE
(fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Tue 16-May-06 16:09 by kellythw
<more output removed for brevity>
```

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」。

Cisco Unified Communications Manager はまたいくつかのこれらの脆弱性からそれらが異なる Cisco バグ ID によってトラッキングされるが、影響を受けます。 Cisco Unified Communications Manager のための友達 Security Advisory は 924-cucm で利用できます。

脆弱性を含んでいないことが確認された製品

SIP アプリケーション層ゲートウェイ（ALG）はこれらの脆弱性から IOS ネットワーク アドレス変換（NAT）および Cisco IOS のファイアウォール特性によって使用される影響を受けない。

Cisco IOS XR が稼働している Cisco デバイスは該当しません。

Cisco Unified Communications Manager を除いて、その他のCisco製品はこのアドバイザリに説明がある問題に脆弱であるために現在知られていません。

詳細

SIP はインターネットのような IP ネットワークを渡る音声およびビデオ呼び出しを管理するのに使用される普及したシグナリング プロトコルです。 SIP はコールセットアップおよび終了のすべての側面を処理する役割があります。 音声およびビデオは SIP が処理するが、プロトコルがコールセットアップおよび終了を必要とする他のアプリケーションのために取り扱うために適用範囲が広いセッションのほとんどの一般的なタイプです。 SIP 呼出し シグナリングは TCP （5060）ポート、または TLS （根本的な転送 プロトコルとして 5061）TCPポート UDP （5060）ポートを使用できます。

多重サービス拒否の脆弱性は Cisco IOS の SIP 実装にあります。 いずれの場合も脆弱性は有効な SIP メッセージの処理によって引き起こすことができます。

メモリリーク の 脆弱性

CSCse56800 により（登録ユーザのみ）影響を受けたデバイスでメモリリークを引き起こします。 メモリリークは有効な SIP メッセージの特定の種類の処理によって Cisco IOSデバイスがまだ動作しても引き起こされ、結局すべての音声 サービスのアベイラビリティを破壊するかもしれません。 この脆弱性よくある脆弱性および公開（CVE）ID CVE-2008-3799 は割り当てられました。

デバイスのリロード脆弱性

次の脆弱性は Cisco IOSデバイスのリロードにいくつかの特定および有効な SIP メッセージを処理している間導く場合があります:

- CVE ID CVE-2008-3800 を割り当てられる CSCsg91306 （登録ユーザのみ）
- CVE ID CVE-2008-3801 を割り当てられる CSCsl62609 （登録ユーザのみ）

- CVE ID CVE-2008-3802 を割り当てられる CSCsk42759 （登録ユーザのみ）

回避策

影響を受けた Cisco IOSデバイスが Voice over IP サービスおよび従って必要があれば SIP を提供するリストされた脆弱性のどれも持っています回避策をそれからディセーブルにすることができません。 これらの脆弱性による影響を制限するために、いくつかの緩和策を適用することを推奨いたします。 その緩和策とは、適切なデバイスのみがルータに接続できるように設定することです。 効果を高めるために、軽減はネットワークエッジのアンチスプーフィング手段とつなぐ必要があります。 SIP が転送 プロトコルとして UDP を使用できるのでこの操作が必要となります。

ネットワーク内のシスコ デバイスに適用可能な他の対応策は、このアドバイザリの付属ドキュメントである『Cisco Applied Mitigation Bulletin』を参照してください。以下のリンクから入手できます。 http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20080924-sip。

ディセーブル SIP リスニングポート

SIP が有効に なるように要求しないデバイスに関しては最も簡単のおよびほとんどの有効な回避策はデバイスで処理する SIP をディセーブルにすることです。 次のコマンドとこれを達成する Cisco IOS 割り当て管理者のバージョン:

```
router>show version
Cisco IOS Software, 7200 Software (C7200-ADVSECURITYK9-M), Version 12.4(6)T2, RELEASE SOFTWARE
(fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Tue 16-May-06 16:09 by kellythw
<more output removed for brevity>
```

警告： この回避策を MGCP か H.323 を処理するデバイスに適用するとき呼出す、デバイスはアクティブ コールが処理されている間処理する SIP を停止することを可能にしません。 このような状況では、この対応策はアクティブ コールが簡潔に停止することができるとき Maintenance ウィンドウの間に設定されるはずです。

この対応策を適用した後、脆弱性が存在する製品で説明されている **show コマンドが** Cisco IOSデバイスがもはや SIP メッセージを処理していないことを確認するのにことを使用されている区分することを推奨します。

コントロール プレーン ポリシング

提供する必要があるデバイスに関しては SIP はそれをです信頼できないソースからのデバイスに SIP トラフィックをブロックするのにコントロール プレーン ポリシング（CoPP）を使用して可能性のある保守します。 Cisco IOS ソフトウェア リリース 12.0S、12.2SX、12.2S、12.3T、12.4、および 12.4T は、CoPP 機能をサポートしています。 デバイスに CoPP を設定して、管理プレーンとコントロール プレーンを保護し、既存のセキュリティ ポリシーおよび設定に従って、

インフラストラクチャのデバイスに送信される承認されたトラフィックだけを明示的に許可することで、インフラストラクチャへの直接攻撃のリスクと効果を最小限に抑えることができます。次の例はネットワークに適応させることができます:

```
router>show version
Cisco IOS Software, 7200 Software (C7200-ADVSECURITYK9-M), Version 12.4(6)T2, RELEASE SOFTWARE
(fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Tue 16-May-06 16:09 by kellythw
<more output removed for brevity>
```

警告： SIP は転送 プロトコルとして UDP を利用できるので容易に信頼された IP アドレスからのこれらのポートに ACL をその割り当て通信敗北させるかもしれない送信側の IP アドレスをスプーフィングすることは可能性のあるです。

上記の CoPP の例では、"permit" アクションであるアクセスコントロールリストエントリ (ACE) に該当し、攻撃である可能性のあるパケットは、policy-map の "drop" 機能により廃棄されますが、一方、"deny" アクション(記載されていません)に該当するパケットは、policy-map の "drop" 機能の影響を受けません。 CoPP 機能の設定および使用のその他の情報は http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.html および http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html で見つけることができます。

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	修理されたリリースの Â Â Â Â Â 可用性

ー リリース		
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	脆弱性あり; first fixed in 12.4	12.4(15)T7 12.4(18c)
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(33)SB2; 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 12.4	12.4(15)T7 12.4(18c)
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; migrate to any release in 12.2S	12.2(33)SB2; 26-SEP-08 で利用可能
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	
12.2IRB	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	Release prior to 12.2(15)MC2c are vulnerable， releases 12.2(15)MC2c and later are not vulnerable; first fixed in 12.4	12.4(15)T7 12.4(18c)
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	
12.2SE	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	

12.2SRA	脆弱性なし	
12.2SRB	脆弱性なし	
12.2SRC	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	
12.2SW	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	
12.2SY	脆弱性なし	
12.2SZ	脆弱性なし	
12.2T	脆弱性あり; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.2TPC	脆弱性あり; contact TAC	
12.2XA	脆弱性なし	
12.2XB	脆弱性あり; first fixed in 12.4	12.4(15)T7 12.4(18c)
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	脆弱性あり; first fixed in 12.4	12.4(15)T7

		12.4(18c)
12.2XN	脆弱性なし	
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	脆弱性あり; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.2XU	脆弱性あり; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.2XV	脆弱性なし	
12.2XW	脆弱性あり; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.2YA	脆弱性あり; first fixed in 12.4	12.4(15)T7 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	脆弱性なし	
12.2YF	脆弱性あり; contact TAC	
12.2YG	脆弱性なし	
12.2YH	脆弱性あり; contact TAC	
12.2YJ	脆弱性あり; contact TAC	
12.2YK	脆弱性なし	
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; contact TAC	
12.2YU	脆弱性あり; contact TAC	
12.2YV	Release prior to 12.2(11)YV1 are	

	vulnerable， releases 12.2(11)YV1 and later are not vulnerable;	
12.2YW	脆弱性あり; contact TAC	
12.2YX	脆弱性なし	
12.2YY	脆弱性あり; contact TAC	
12.2YZ	脆弱性なし	
12.2ZA	脆弱性なし	
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 12.4	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	脆弱性なし	
12.2ZH	脆弱性あり; first fixed in 12.4	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(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	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	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	脆弱性あり; contact TAC	
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(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	脆弱性あり; migrate to any release in 12.2SB	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	脆弱性あり; first fixed in 12.4	12.4(15)T7 12.4(18c)
12.3XS	脆弱性なし	
12.3XU	脆弱性あり; first fixed in 12.4T	12.4(15)T

		7
12.3XW	脆弱性あり; first fixed in 12.3YX	12.3(14)YX13 12.4(15)T7
12.3XX	脆弱性あり; first fixed in 12.4	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)T7 12.4(18c)
12.3YA	脆弱性なし	
12.3YD	脆弱性なし	
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)YG7; 01-OCT-08 で利用可能	12.4(15)T7
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)T7
12.3YM	12.3(14)YM13; 30-SEP-08 で利用可能	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)YX12	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(13f) 12.4(17b) 12.4(18)	12.4(18c)
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(19)MR	12.4(19)MR
12.4SW	脆弱性なし	
12.4T	12.4(15)T4 12.4(20)T 12.4(6)T11	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)XB10	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)XD11; 26-SEP-08 で利用可能	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	脆弱性なし	
12.4XJ	脆弱性あり; first fixed in 12.4T	12.4(15)T7
12.4XK	脆弱性なし	
12.4XL	12.4(15)XL2	12.4(15)XL2
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	脆弱性あり; first fixed in 12.4T	12.4(15)T7
12.4XV	脆弱性あり; contact TAC	
12.4XW	12.4(11)XW7	12.4(11)XW9
12.4XY	12.4(15)XY3	12.4(15)XY4
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

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。

これらの脆弱性は Cisco 内部テストによっておよび弊社販売代理店 要求の処理の間に検出されました。

出典

URL

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

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-September-24	初版リリース

利用規約