Cisco IOSソフトウェア 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-20090325-sip **初公開日 :** 2009-03-25 16:00 **バージョン 1.4 :** Final **CVSSスコア :** 7.8 **回避策 :** No Workarounds available **Cisco バグ ID :** CSCsu11522	CVE-2009-0636

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 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ソフトウェアのセッション開始プロトコル（SIP）実装で存在 する脆弱性。

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デバイスが VOIPサービスのための SIP を実行する必要はない場合、利用可能 な 回避策が脆弱性を SIP をディセーブルにすることから離れて軽減するためにありません。 ただし、緩和技術は脆弱性への公開の制限を助けて利用できます。

このアドバイザリは次のリンクに掲載されます: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-sip。

注: 2009 年 3月 25 日、Cisco IOS セキュリティ アドバイザリによって組み込まれる書は 8 つのセキュリティ アドバイザリが含まれています。 アドバイザリすべては Cisco IOSソフトウェア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の脆弱性を解決する。

各ドキュメントへのリンクは次のとおりです。

- Cisco IOS cTCP サービス拒否の脆弱性
  325-ctcp

- Cisco IOSソフトウェア倍数は IP ソケット脆弱性を特色にします
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ip

- Cisco IOSソフトウェア モバイル IP およびモービル IPv6 脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-mobileip

- Cisco IOSソフトウェア Secure Copy（SCP） 特権 拡大脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-scp

- Cisco IOSソフトウェア Session Initiation Protocol（SIP） サービス拒否の脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-sip

- Cisco IOSソフトウェア複数の機能によって細工 される TCP シーケンス脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-tcp

- Cisco IOSソフトウェア複数の機能 巧妙に細工された UDP パケットの脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-udp

- Cisco IOSソフトウェア WebVPN および SSLVPN 脆弱性
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-webvpn

該当製品

この脆弱性は有効に なる SIP 音声 サービスを用いる実行するデバイス Cisco IOSソフトウェアだけに影響を与えます。

脆弱性のある製品

SIP メッセージを処理する影響を受けた Cisco IOS ソフトウェア バージョンを実行するCiscoデバイスは影響を受けています。 この脆弱性のための唯一の要件は設定された VoIP 機能の一部としてこと Cisco IOSデバイス プロセス SIP メッセージです。 これが 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ないことに注目して下さい。

Cisco IOSソフトウェア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。

コマンド **dial-peer voice** を通ってダイヤル ピアを作成することは SIP プロセスを開始し、Cisco IOSデバイスを SIP メッセージを処理し始めさせます。 さらに、Cisco Unified Communications Manager Express 内の複数の機能は、一度設定された ephone のようなまた、自動的にデバイスが SIP メッセージを処理し始めます SIP プロセスを開始します。 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
 ...
!
```

注: Cisco IOSソフトウェアのより古いバージョンは Cisco IOSソフトウェアが SIP オペレーションのために設定されないで SIP メッセージを処理しました不具合から影響を受けました。 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コマンド **show processes を**使用できます **|** Cisco IOSソフトウェアが 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ために **SIP を含んで下さい。** 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
```

警告： 複数の方法があるので Cisco IOSソフトウェアを実行するデバイスはそれ推奨されますこと **show processes** SIP メッセージを処理し始めることができます **| SIP** コマンドをデバイスが特定の設定コマンドことをの存在に頼るかわりに SIP メッセージを処理しているかどうか判別するのに使用されています**含んで下さい。**

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

SIP アプリケーション層ゲートウェイ（ALG）はこの脆弱性から、Cisco IOSソフトウェアの Cisco IOS NAT およびファイアウォール特性によって使用される、影響を受けません。

Cisco IOS XE ソフトウェアおよび Cisco IOS XR ソフトウェアを実行している Ciscoデバイスは影響を受けていません。

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

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す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、プロトコルに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を取り扱う柔軟性がある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。

Cisco IOSソフトウェアの SIP 実装で存在 する サービス拒否（DoS）脆弱性。 この脆弱性は特定および有効な SIP メッセージの処理によって引き起こされます。

この脆弱性 Cisco バグ ID **CSCsu11522**（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-2009-0636 は割り当てられました。

注: アドバイザリ Cisco IOSソフトウェア倍数機能 IP ソケット脆弱性および Cisco IOSソフトウェア複数の機能によって細工 される UDP パケットの脆弱性に、Cisco IOS アドバイザリのこの

バンドルの両方の一部説明がある、脆弱性はまた SIP オペレーションに影響を与えるかもしれません。

回避策

影響を受けた Cisco IOSデバイスが VOIPサービスのために SIP を必要とする場合、SIP は無効である場合もないし従って、対応策は見つかりません。 ユーザは脆弱性への公開の制限を助ける緩和技術を適用するように助言されます。 軽減は正当 な デバイスだけルータに接続するようにすることで構成されています。 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 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: 」Cisco IOS SIP および巧妙に細工された UDP 脆弱性の識別し、次の位置で利用可能である軽減不正利用、: http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20090325-sip-and-udp。

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ソフトウェア割り当て管理者のバージョン:

```
sip-ua
 no transport udp
 no transport tcp
```

警告： この回避策をメディア ゲートウェイ コントロール プロトコル（MGCP）または H.323 呼び出しを処理しているデバイスに適用するとき、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 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、管理者はこのアドバイザリの Affected Products セクションに記述されているように **show コマンドを**、使用するように助言されます。

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 Release 12.0S、12.2SX、12.2S、12.3T、12.4、および 12.4T サポート CoPP 機能。 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:

```
!-- The 192.168.1.0/24 network and the 172.16.1.1 host are trusted. !-- Everything else is not trusted. The following access list is used !-- to determine what traffic needs to be dropped by a control plane !-- policy (the CoPP feature.) If the access list matches (permit) !-- then traffic will be dropped and if the access list does not !-- match (deny) then traffic will be processed by the router. access-list 100 deny udp 192.168.1.0 0.0.0.255 any eq 5060 access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 5060 access-list 100 deny tcp 192.168.1.0 0.0.0.255 any eq 5061 access-list 100 deny udp host 172.16.1.1 any eq 5060 access-list 100 deny tcp host 172.16.1.1 any eq 5060 access-list 100 deny tcp host 172.16.1.1 any eq 5061 access-list 100 permit udp any any eq 5060 access-list 100 permit tcp any any eq 5060 access-list 100 permit tcp any any eq 5061 !-- Permit (Police or Drop)/Deny (Allow) all other Layer3 and Layer4 !-- traffic in accordance with existing security policies and !-- configurations for traffic that is authorized to be sent !-- to infrastructure devices. !-- Create a Class-Map for traffic to be policed by !-- the CoPP feature. class-map match-all drop-sip-class match access-group 100 !-- Create a Policy-Map that will be applied to the !-- Control-Plane of the device. policy-map drop-sip-traffic class drop-sip-class drop !-- Apply the Policy-Map to the Control-Plane of the !-- device. control-plane service-policy input drop-sip-traffic
```

警告： SIP は転送 プロトコルとして UDP を使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アクセスコントロール アクセス・コントロール・リスト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。

CoPP 上の例では、「拒否」操作を一致するパケットは policy-map ドロップする 機能から（示されていない）影響を受けないが policy-map 「ドロップする」機能によって廃棄されるこれらのパケットの「割り当て」アクションの結果を用いる潜在的なエクスプロイト パケット一致する アクセス制御エントリ（ACE）その。 CoPP 機能の設定および使用のその他の情報は http://www.cisco.com/web/about/security/intelligence/coppwp_gs.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。

注: が理由で CSCsu11522 に加えておよび SIP オペレーションの影響、「Cisco Security Advisory からの Ciscoバグ CSCsk64158 が、トラッキングする修正済みソフトウェアのこの表は脆弱性を考慮に入れます: 巧妙に細工された UDP パケットは複数の Cisco IOS機能に」影響を与えます（表が脆弱性を考慮に入れない http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-udp.) は「Cisco Security Advisory によって表われました: TLS 上の SIP に影響を与えるかもしれない複数の Cisco IOS機能に」影響を与える Cisco IOS IP ソケット脆弱性。

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	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0DA	脆弱性あり; first fixed in 12.2DA	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0DB	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0DC	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0S	12.0(32)S12	12.0(32)S12
12.0SC	脆弱性あり; first fixed in 12.0S	12.0(32)S12
12.0SL	脆弱性あり; first fixed in 12.0S	12.0(32)S12
12.0SP	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a);

		05-JUN-2009 で利用可能
12.0ST	脆弱性あり; first fixed in 12.0S	12.0(32)S12
12.0SX	脆弱性あり; first fixed in 12.0S	12.0(32)S12
12.0SY	12.0(32)SY8	12.0(32)SY8
12.0SZ	脆弱性あり; first fixed in 12.0S	12.0(32)S12
12.0T	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0W	脆弱性あり; contact TAC	
12.0WC	脆弱性あり; contact TAC	
12.0WT	脆弱性なし	
12.0XA	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XB	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XC	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XD	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XE	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XF	脆弱性なし	
12.0XG	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利

		用可能
12.0XH	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XI	Release prior to 12.0(4)XI2 are vulnerable， releases 12.0(4)XI2 and later are not vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XJ	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XK	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XL	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XM	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XN	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XQ	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XR	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XS	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利

		用可能
12.0XT	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.0XV	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
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**
12.1	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1AA	脆弱性あり; contact TAC	
12.1AX	脆弱性あり; first fixed in 12.2SE	12.2(44)SE6
12.1AY	脆弱性あり; first fixed in 12.1EA	12.1(22)EA13 12.2(44)SE6
12.1AZ	脆弱性あり; first fixed in 12.1EA	12.1(22)EA13 12.2(44)SE6
12.1CX	脆弱性あり; contact TAC	
12.1DA	脆弱性あり; contact TAC	
12.1DB	脆弱性あり; contact TAC	
12.1DC	脆弱性あり; contact TAC	
12.1E	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF16
12.1EA	12.1(22)EA13	12.1(22)EA13
12.1EB	脆弱性あり; contact TAC	
12.1EC	脆弱性あり; first fixed in 12.3BC	12.2(33)SCB1 12.3(23)BC6
12.1EO	脆弱性あり; contact TAC	
12.1EU	脆弱性あり; first fixed in 12.2SG	12.2(31)SGA9

12.1EV	脆弱性あり; contact TAC	
12.1EW	脆弱性あり; 12.2SGA への移行する	12.2(31)SGA9
12.1EX	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1EY	脆弱性あり; contact TAC	
12.1EZ	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF16
12.1GA	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1GB	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1T	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XA	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XB	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XC	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XD	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XE	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利

		用可能
12.1XF	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XG	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XH	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XI	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XJ	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XL	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XM	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XP	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XQ	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XR	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利

		用可能
12.1XS	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XT	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XU	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XV	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XW	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XX	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XY	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1XZ	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1YA	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1YB	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利

		用可能
12.1YC	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1YD	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1YE	Release prior to 12.1(5)YE6 are vulnerable， releases 12.1(5)YE6 and later are not vulnerable; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1YF	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1YH	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.1YI	脆弱性あり; contact TAC	
12.1YJ	脆弱性あり; first fixed in 12.1EA	12.1(22)EA13 12.2(44)SE6
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	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2B	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.2BC	脆弱性あり; 12.2SCB または 12.3BC への移行する	12.2(33)SCB1 12.3(23)BC6

12.2BW	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2BX	脆弱性あり; 12.2SB への移行する	12.2(33)SB4
12.2BY	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2BZ	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2CX	脆弱性あり; 12.2SCB または 12.3BC への移行する	12.2(33)SCB1 12.3(23)BC6
12.2CY	脆弱性あり; 12.2SCB または 12.3BC への移行する	12.2(33)SCB1 12.3(23)BC6
12.2CZ	脆弱性あり; first fixed in 12.2SB	12.2(33)SB4
12.2DA	12.2(12)DA14; 30-JUL-2009 で利用可能	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2DD	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2DX	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2EW	脆弱性あり; first fixed in 12.2SG	12.2(31)SGA9
12.2EWA	脆弱性あり; first fixed in 12.2SG	12.2(31)SGA9
12.2EX	脆弱性あり; first fixed in 12.2SE	12.2(44)SE6
12.2EY	12.2(44)EY	12.2(44)SE6

12.2EZ	脆弱性あり; first fixed in 12.2SE	12.2(44)SE6
12.2FX	脆弱性あり; first fixed in 12.2SE	12.2(44)SE6
12.2FY	脆弱性あり; first fixed in 12.2SE	12.2(44)SE6
12.2FZ	脆弱性あり; first fixed in 12.2SE	12.2(44)SE6
12.2IRA	脆弱性あり; first fixed in 12.2SRC	12.2(33)SRC4; 18-MAY-2009 で利用可能
12.2IRB	脆弱性あり; first fixed in 12.2SRC	12.2(33)SRC4; 18-MAY-2009 で利用可能
12.2IXA	脆弱性あり; migrate to any release in 12.2IXH	12.2(18)IXH; 31-MAR-2009 で利用可能
12.2IXB	脆弱性あり; migrate to any release in 12.2IXH	12.2(18)IXH; 31-MAR-2009 で利用可能
12.2IXC	脆弱性あり; migrate to any release in 12.2IXH	12.2(18)IXH; 31-MAR-2009 で利用可能
12.2IXD	脆弱性あり; migrate to any release in 12.2IXH	12.2(18)IXH; 31-MAR-2009 で利用可能
12.2IXE	脆弱性あり; migrate to any release in 12.2IXH	12.2(18)IXH; 31-MAR-2009 で利用可能
12.2IXF	脆弱性あり; migrate to any release in 12.2IXH	12.2(18)IXH; 31-MAR-2009 で利用可能
12.2IXG	脆弱性あり; migrate to any release in 12.2IXH	12.2(18)IXH; 31-MAR-2009 で利用可能
12.2JA	脆弱性なし	
12.2JK	脆弱性なし	
12.2MB	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-

		2009 で利用可能
12.2MC	12.2(15)MC2m	12.2(15)MC2m
12.2S	脆弱性あり; first fixed in 12.2SB	12.2(33)SB4
12.2SB	12.2(28)SB13 12.2(31)SB14 12.2(33)SB3	12.2(33)SB4
12.2SBC	脆弱性あり; first fixed in 12.2SB	12.2(33)SB4
12.2SCA	脆弱性あり; first fixed in 12.2SCB	12.2(33)SCB1
12.2SCB	12.2(33)SCB1	12.2(33)SCB1
12.2SE	12.2(50)SE 12.2(46)SE2 12.2(44)SE5	12.2(44)SE6
12.2SEA	脆弱性あり; first fixed in 12.2SE	12.2(44)SE6
12.2SEB	脆弱性あり; first fixed in 12.2SE	12.2(44)SE6
12.2SEC	脆弱性あり; first fixed in 12.2SE	12.2(44)SE6
12.2SED	脆弱性あり; first fixed in 12.2SE	12.2(44)SE6
12.2SEE	脆弱性あり; first fixed in 12.2SE	12.2(44)SE6
12.2SEF	脆弱性あり; first fixed in 12.2SE	12.2(44)SE6
12.2SEG	脆弱性あり; first fixed in 12.2SE	12.2(44)SE6
12.2SG	12.2(50)SG	12.2(52)SG; 15-MAY-2009 で利用可能
12.2SGA	12.2(31)SGA9	12.2(31)SGA9
12.2SL	脆弱性なし	
12.2SM	脆弱性あり; contact TAC	
12.2SO	脆弱性あり; contact TAC	
12.2SQ	12.2(44)SQ1	
12.2SRA	脆弱性あり; first fixed in 12.2SRC	12.2(33)SRD1 12.2(33)SRC4; 18-MAY-2009 で利用可能

12.2SRB	脆弱性あり; first fixed in 12.2SRC	12.2(33)SRC4; 18-MAY-2009 で利用可能 12.2(33)SRD1 12.2(33)SRB5a; 3-April-2009 で利用可能
12.2SRC	12.2(33)SRC4; 18-MAY-2009 で利用可能	12.2(33)SRC4; 18-MAY-2009 で利用可能
12.2SRD	脆弱性なし	
12.2STE	脆弱性あり; contact TAC	
12.2SU	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
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	
12.2SVE	脆弱性あり; contact TAC	
12.2SW	脆弱性あり; contact TAC	
12.2SX	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF16
12.2SXA	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF16
12.2SXB	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF16
12.2SXD	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF16
12.2SXE	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF16
12.2SXF	12.2(18)SXF16	12.2(18)SXF16
12.2SXH	12.2(33)SXH5; 20-APR-2009 で利用可能	12.2(33)SXH5; 20-APR-2009 で利用可能
12.2SXI	脆弱性なし	
12.2SY	脆弱性あり; first fixed in 12.2SB	12.2(33)SB4
12.2SZ	脆弱性あり; first fixed in 12.2SB	12.2(33)SB

		4
12.2T	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2TPC	脆弱性あり; contact TAC	
12.2XA	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XB	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XC	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XD	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XE	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XF	脆弱性あり; 12.2SCB または 12.3BC への移行する	12.2(33)SCB1 12.3(23)BC6
12.2XG	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XH	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XI	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利

		用可能
12.2XJ	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XK	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XL	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XM	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XN	脆弱性あり; first fixed in 12.2SRC	12.2(33)SB4 12.2(33)SRD1
12.2XNA	脆弱性あり; migrate to any release in 12.2SRD	12.2(33)SRD1
12.2XNB	12.2(33)XNB1	12.2(33)XNB3
12.2XNC	脆弱性なし	
12.2XO	12.2(46)XO	12.2(46)XO
12.2XQ	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XR	脆弱性なし	
12.2XS	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XT	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XU	脆弱性あり; first fixed in 12.4	12.4(18e)

		12.4(23a); 05-JUN-2009 で利用可能
12.2XV	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2XW	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2YA	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
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	脆弱性あり; contact TAC	
12.2YF	脆弱性あり; contact TAC	
12.2YG	脆弱性あり; contact TAC	
12.2YH	脆弱性あり; contact TAC	
12.2YJ	脆弱性あり; contact TAC	
12.2YK	脆弱性あり; contact TAC	
12.2YL	脆弱性あり; contact TAC	
12.2YM	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.2YN	脆弱性あり; contact TAC	
12.2YO	脆弱性あり; contact TAC	
12.2YP	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2YQ	脆弱性あり; contact TAC	
12.2YR	脆弱性あり; contact TAC	
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	脆弱性あり; contact TAC	

12.2YW	脆弱性あり; contact TAC	
12.2YX	脆弱性あり; contact TAC	
12.2YY	脆弱性あり; contact TAC	
12.2YZ	脆弱性あり; contact TAC	
12.2ZA	脆弱性あり; first fixed in 12.2SXF	12.2(18)SXF16
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(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.2ZF	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.2ZG	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.2ZH	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
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	脆弱性あり; first fixed in 12.2SXH	12.2(33)SXH5; 20-APR-2009 で利用可能
12.2ZX	脆弱性あり; first fixed in 12.2SB	12.2(33)SB4
12.2ZY	脆弱性あり; contact TAC	
12.2ZYA	12.2(18)ZYA1	12.2(18)ZYA1
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(18e) 12.4(23a);

		05-JUN-2009 で利用可能
12.3B	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3BC	12.3(23)BC6	12.3(23)BC6
12.3BW	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
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	脆弱性あり; contact TAC	
12.3JX	脆弱性なし	
12.3T	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3TPC	脆弱性あり; contact TAC	
12.3VA	脆弱性あり; contact TAC	
12.3XA	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.3XB	脆弱性あり; contact TAC	
12.3XC	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3XD	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3XE	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a);

		05-JUN-2009 で利用可能
12.3XF	脆弱性あり; contact TAC	
12.3XG	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3XI	脆弱性あり; first fixed in 12.2SB	12.2(33)SB4
12.3XJ	脆弱性あり; first fixed in 12.3YX	12.3(14)YX14
12.3XK	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3XL	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3XQ	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3XR	脆弱性あり; first fixed in 12.4	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.3XS	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3XU	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3XW	脆弱性あり; first fixed in 12.3YX	12.3(14)YX14
12.3XX	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能

12.3XY	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3XZ	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YA	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YD	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YF	脆弱性あり; first fixed in 12.3YX	12.3(14)YX 14
12.3YG	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YH	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YI	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YJ	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YK	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YM	12.3(14)YM13	12.3(14)YM 13
12.3YQ	脆弱性あり; first fixed in 12.4T	12.4(22)T1

		12.4(15)T9; 29-APR-2009 で利用可能
12.3YS	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YT	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YU	脆弱性あり; first fixed in 12.4XB	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.3YX	12.3(14)YX14	12.3(14)YX14
12.3YZ	脆弱性あり; contact TAC	
12.3ZA	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-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(18e) 12.4(23) 12.4(23a); 05-JUN-2009 で利用可能	12.4(18e) 12.4(23a); 05-JUN-2009 で利用可能
12.4JA	脆弱性なし	
12.4JDA	脆弱性なし	
12.4JK	脆弱性なし	
12.4JL	脆弱性なし	
12.4JMA	脆弱性あり; contact TAC	
12.4JMB	脆弱性あり; contact TAC	
12.4JX	脆弱性なし	
12.4MD	12.4(11)MD7	12.4(11)MD7
12.4MR	12.4(19)MR1	12.4(19)MR2

12.4SW	脆弱性あり; contact TAC	
12.4T	12.4(20)T2 12.4(15)T8 12.4(22)T 12.4(15)T9; 29-APR-2009 で利用可能	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XA	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XB	12.4(15)T8 12.4(20)T2 12.4(15)T9; 29-APR-2009 で利用可能	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XC	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XD	12.4(4)XD12; 27-MAR-2009 で利用可能	12.4(4)XD12; 27-MAR-2009 で利用可能
12.4XE	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XF	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XG	12.4(15)T8 12.4(20)T2	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XJ	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XK	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能

12.4XL	12.4(15)XL4	12.4(15)XL4
12.4XM	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XN	脆弱性あり; contact TAC	
12.4XP	脆弱性あり; contact TAC	
12.4XQ	12.4(15)XQ2	12.4(15)XQ2
12.4XR	12.4(15)XR4	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XT	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XV	脆弱性あり; contact TAC	
12.4XW	12.4(11)XW10	12.4(11)XW10
12.4XY	脆弱性あり; first fixed in 12.4T	12.4(22)T1 12.4(15)T9; 29-APR-2009 で利用可能
12.4XZ	12.4(15)XZ2	12.4(15)XZ2
12.4YA	12.4(20)YA2	12.4(20)YA3
12.4YB	脆弱性なし	
12.4YD	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。

この脆弱性はお客様からのお問い合わせへの対応の際に発見されました。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-sip

改訂履歴

リビジョン 1.4	2009-June-26	March/09 によって結合される修正済みソフトウェア 表への取除かれた参照。
リビジョン 1.3	2009-June-1	リリース 12.4(23a) のための更新済期待された公共有効 日付。
リビジョン 1.2	2009-May-1	リリース 12.4(23a) のための更新済期待された公共有効 日付。
リビジョン 1.1	2009-April-03	リリース 12.2XR、12.4JL、12.4JK、12.4JX、12.4JDA、12.4JA、12.3JX、12.3JK、12.3JEC、12.3JEB、12.3JEA、12.3JA、12.2JA および 12.2JK は脆弱であるために確認されました。 調節された修正済みソフトウェア 表それに応じて。
リビジョン 1.0	2009-March-25	初版リリース

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。