Cisco IOSソフトウェア Secure Copy（SCP）特権 拡大脆弱性

Critical

アドバイザリーID : cisco-sa-20090325-scp
初公開日 : 2009-03-25 16:00
バージョン 1.3 : Final
CVSSスコア : 9.0
回避策 : No Workarounds available
Cisco バグ ID : CSCsv38166

CVE-2009-0637

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ソフトウェアの Secure Copy（SCP）実装のサーバ側は接続された Command Line Interface（CLI）ビューの認証済みユーザがどんなユーザがであるためにするために許可されるかに関係なく SCP サーバ、設定される CLI ビュー設定ごとの Cisco IOSデバイスに出入してファイルを転送することを可能にする可能性がある脆弱性が含まれています。 この脆弱性はユーザに接続される CLI ビューがそれを可能にしなくても有効 な ユーザがデバイスのファイル システムであらゆるファイルに、デバイスの保存された 設定および Cisco IOSイメージ ファイルを含んで取得するか、または書くことを可能にする可能性があります。 この設定ファイルには、パスワードなどの機密情報が含まれている場合があります。

Cisco IOS SCP サーバはデフォルトでディセーブルにされるオプションのサービスです。 CLI 意見はまたデフォルトでディセーブルにされる Cisco IOS 役割ベース CLI アクセス機能の基本的 なコンポーネントです。 Cisco IOS SCP サーバをイネーブルに設定するために明確に設定されないまたはそれを使用するために設定されるが、使用しない役割ベース CLI アクセスをデバイスはこの脆弱性から、影響を受けません。

この脆弱性は Cisco IOS SCP クライアント機能に適用しません。

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。

これらのサービスが管理者によって必要とされない場合 SCP サーバか CLI ビュー機能をディセーブルにすることから離れてこの脆弱性のために利用可能 な 回避策がありません。

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-scp。

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

脆弱性のある製品

SCP サーバの機能性を提供するために設定され役割ベース ACL アクセスを使用するために設定される該当する Cisco IOS ソフトウェア リリースを実行する Ciscoデバイスはこの問題から影響を受けます。

脆弱 な Cisco IOS ソフトウェア リリースを実行するデバイスは設定が次に類似したである場合影響を受けています:

```
parser view <view name>
 <Definition of the CLI view>
!
username <user ID> view <view name> secret <some secret>
!
ip scp server enable
```

上のコンフィギュレーション の 断片では、**パーサー ビュー** コマンドはどんなコマンドを実行そのビューのユーザができるか規定 する意見を定義したものです。 **username コマンドは**ローカルユーザを定義し、**View キーワード**によって、ユーザに以前に定義された意見を接続します。 そして最終的に、**IP SCP サーバ enable コマンドは** Cisco IOS SCP サーバをイネーブルに設定します。

username コマンドの不在は CLI ビューの名前が認証、許可、アカウンティング（AAA） サーバによって cli ビュー**名前**アトリビュートの利用によって供給することができるのでデバイス・コンフィギュレーションがこの脆弱性から影響を受けないことを保証しません。

注: ユーザに接続される CLI ビューは AAAサーバによって供給することができます。 デバイス・コンフィギュレーションを確認するために点検することはこの脆弱性からそれ影響を受けたかどうか SCP サービスが有効に なるかどうか確認してがより適切な（**IP SCP サーバ enabled コマンド**）およびかどうかそこにである定義される CLI 意見とき（**パーサー ビュー** コマンド）。

Cisco IOS SCP サーバおよび役割ベース CLI アクセス機能はデフォルトでディセーブルにされます。

SCP サーバの機能性は暗号化可能なイメージだけで利用できます。 暗号化可能なイメージはイメージ名で "k8" か "k9" が、たとえば、"C7200-ADVSECURITYK9-M" 含まれているイメージです。 暗号化可能なイメージを実行しないデバイスは脆弱ではないです。 デバイスが暗号化可能なイメージを、**IP SCP サーバ enable コマンド**の設定の存在、CLI 意見デバイスは影響を受けていたかどうかあるかどうか（**パーサー ビュー** コマンド）の存在実行すれば、およびこれらの意見に接続したユーザが（ローカルか遠隔）確認すれば。

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。

Cisco IOS XE ソフトウェアはまたこの脆弱性から影響を受けます。

脆弱性を含んでいないことが確認された製品

Cisco IOSソフトウェアを実行しない Ciscoデバイスは影響を受けていません。

有効に なる SCP サーバ 機能を備えていないまたは機能を利用するが、ない有効に なる 役割ベース CLI 機能が Cisco IOSデバイスは影響を受けていません。

Cisco IOS XR ソフトウェア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

システム間のファイルの転送を可能にする SCP はリモート コピー（RCP）プロトコルと同じようなプロトコルです。 SCP と RCP の大きな違いは、SCP では、認証を含む転送セッションのすべての部分が暗号化された形式で実行されることであり、このために SCP の方が RCP より安

全です。 SCP は Secure Shell (SSH; セキュア シェル) プロトコルを利用し、デフォルトでは TCP ポート 22 を使用します。

役割ベース CLI アクセス機能はネットワーク管理者が「意見」を定義することを可能にします。ビューは作戦 指揮および Cisco IOSソフトウェア EXEC および設定 (構成) モード コマンドに選択的か部分的なアクセスを提供する設定機能のセットです。 ビューは Cisco IOS Command Line Interface （ CLI) および構成情報にユーザアクセスを制限します; すなわち、ビューはどんなコマンドが許可され、どんな構成情報が目に見えるか定義できます。 役割ベース CLI アクセス機能に関する詳細については、参照 http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtclivws.html。

Cisco IOSソフトウェアの SCP 実装のサーバ側は接続された Command Line Interface （ CLI) ビューの認証済みユーザがどんなユーザがであるためにするために許可されるかに関係なく SCP サーバ、設定される CLI ビュー設定ごとの Cisco IOSデバイスに出入してファイルを転送することを可能にする脆弱性が含まれています。 この脆弱性は認証済みユーザがデバイスの保存された設定および Cisco IOSイメージ ファイルを含むデバイスのファイル システムであらゆるファイルに、取得するか、または書くことを可能にする可能性があります。 この設定ファイルには、パスワードなどの機密情報が含まれている場合があります。

CLI ビューに Affected Products セクションで、制限されるユーザは SCP のデバイス・コンフィギュレーションに書くのに使用によって表記される影響を受けた設定では特権を上げることができます。 AAAサーバことをからのアトリビュート cli ビュー**名前を**渡すことによるユーザを口ーカルデータベースの (**ユーザ名 <user name> ビュー...**コマンドによって)、または定義した場合ビューがユーザに接続することができることに注目して下さい。

この脆弱性は認証 バイパスを可能にしません; ログオン資格情報は確認され、有効なユーザ名およびパスワードが提供される場合その時だけアクセスは認められます。 この脆弱性が悪用されると、**許可**がバイパスされる可能性があります。

この脆弱性 Cisco バグ ID **CSCsv38166** （ 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-2009-0637 は割り当てられました。

回避策

Cisco IOS SCP サーバの機能性が必要とされなければこの文書に説明がある脆弱性は SCP サーバか CLI ビュー機能をディセーブルにすることによって軽減することができます。 SCP サーバはグローバル コンフィギュレーション モードの次のコマンドの実行によってディセーブルにすることができます:

```
no ip scp server enable
```

SCP サーバが操作上問題が無効原因である場合もない場合回避策はありません。 この脆弱性によって提起されるリスクは http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml で

Cisco IOSデバイス」を堅くするために「Cisco ガイドで詳述される最良 の 方法に続くことによって軽減することができます。 この脆弱性を解決するために適切なソリューションのための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を参照して下さい。

この属性の性質上、デバイスへのアクセスを特定の IP アドレスまたはサブネットワークに制限する Access Control List (ACL; アクセス コントロール リスト) や Control Plane Policing (CoPP; コントロール プレーン ポリシング) などのネットワークのベスト プラクティスは、有効ではない場合があります。 アクセスが特定の IP アドレスかサブネットワークに既に認められている場合、低い特権のユーザはユーザがこの脆弱性を不正利用することを可能にするデバイスとの SCP セッションを設定できます。

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-	**First Fixed Release (修正された最初のリリース)**	**推奨リリース**

Based Releases		
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	脆弱性あり; migrate to any release in 12.2SEG	12.2(44)SE6
12.2EY	脆弱性あり; first fixed in 12.2SE	12.2(44)SE6
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	脆弱性なし	

12.2SB	12.2(33)SB4	12.2(33)SB4
12.2SBC	脆弱性なし	
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(44)SE6	12.2(44)SE6
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	12.2(52)SG; 15-MAY-2009 で利用可能	12.2(52)SG; 15-MAY-2009 で利用可能
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	脆弱性あり; contact TAC	
12.2SRA	脆弱性なし	
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)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	12.2(33)SRD1	12.2(33)SRD1
12.2STE	脆弱性あり; contact TAC	
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	12.2(33)SXI1	12.2(33)SXI1
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 12.2SRC	12.2(33)SB4 12.2(33)SRD1 12.2(33)SRC4; 18-MAY-2009 で利用可能
12.2XNA	脆弱性あり; first fixed in 12.2SRD	12.2(33)SRD1 12.2(33)SRC4; 18-MAY-2009 で利用可能
12.2XNB	12.2(33)XNB3	12.2(33)XNB3
12.2XNC	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	脆弱性なし	
12.3B	脆弱性なし	
12.3BC	脆弱性なし	
12.3BW	脆弱性なし	
12.3EU	脆弱性なし	
12.3JA	脆弱性あり; contact TAC	
12.3JEA	脆弱性あり; contact TAC	
12.3JEB	脆弱性あり; contact TAC	
12.3JEC	脆弱性あり; contact TAC	
12.3JK	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
12.3JL	脆弱性なし	
12.3JX	脆弱性あり; contact TAC	
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	脆弱性なし	
12.3VA	脆弱性あり; contact TAC	
12.3XA	脆弱性なし	
12.3XB	脆弱性なし	
12.3XC	脆弱性なし	
12.3XD	脆弱性なし	
12.3XE	脆弱性なし	
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	脆弱性なし	
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)YX14
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)YM13
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 12.4T	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(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	脆弱性あり; contact TAC	
12.4JDA	脆弱性あり; contact TAC	
12.4JK	脆弱性あり; contact TAC	
12.4JL	脆弱性あり; contact TAC	
12.4JMA	脆弱性あり; contact TAC	
12.4JMB	脆弱性あり; contact TAC	
12.4JX	脆弱性あり; contact TAC	
12.4MD	12.4(11)MD7	12.4(11)MD7
12.4MR	12.4(19)MR2	12.4(19)MR2
12.4SW	脆弱性あり; contact TAC	
12.4T	12.4(24)T 12.4(20)T2 12.4(22)T1 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	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
12.4XC	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(20)T2 12.4(22)T1	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	Release prior to 12.4(15)XL4 are vulnerable， releases 12.4(15)XL4 and later are not vulnerable;	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	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
12.4XT	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 Kevin Graham によって Cisco に報告されました。 Cisco はこの脆弱性を報告し、脆弱性の調整された公開の方に私達とはたらくことに氏に感謝することを Graham 望みます。

出典

URL

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

改訂履歴

リビジョン 1.3	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 1.2	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 1.1	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 1.0	2009-March-25	初版リリース

利用規約

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。