Cisco IOSソフトウェア 認証プロキシ脆弱性

High

アドバイザリーID : cisco-sa-20090923-auth-proxy

初公開日 : 2009-09-23 16:00

バージョン 1.1 : Final

CVSSスコア : 7.1

回避策 : No Workarounds available

Cisco バグ ID : CSCsy15227

CVE-2009-2863

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

HTTP のための認証プロキシで、Web 認証か同意機能設定される、Cisco IOS® ソフトウェアは非認証セッションが認証 プロキシサーバをバイパスするか、または同意 Web ページをバイパスするようにするかもしれない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。

この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 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-auth-proxy 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

実行するデバイスは Cisco IOSソフトウェアのバージョンに影響を与え、HTTP または Web 認証または同意機能のための認証プロキシで設定されて脆弱 でであって下さい。

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 Â©) 1986-2008 by cisco Systems, Inc.
 Compiled Mon 17-Mar-08 14:39 by dchih

 <output truncated>
```

以下の例は、Cisco 製品にて、IOSリリース 12.4(20)T が稼動し、そのイメージ名が C1841-ADVENTERPRISEK9-M であることを示しています:

```
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 Â©) 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。

デバイスが HTTP のための認証プロキシ、Web 認証か承諾機能で設定されたかどうか確認するために、デバイスにログイン し、**show running-config コマンドを**発行して下さい。

次の例はプロキシ ルール名前 example_auth_proxy_name の下で ip auth-proxy を使用してファイアウォール 認証プロキシ サービスを示したものです:

```
Router#show running-config
<output truncated>
 ! ! Set up the aaa new model to use the authentication proxy. ! aaa authorization auth-proxy
default group ! ! Apply a name to the authentication proxy configuration rule. ! ip auth-proxy
name example_auth_proxy_name http ! ! Apply the authentication proxy rule at an interface. !
interface e0 ip auth-proxy example_auth_proxy_name ! <output truncated>
```

次の例は IP 許可コマンドを使用してプロキシ ルール名前 example_auth_proxy_name の下で HTTP のために、動作しているファイアウォール 認証プロキシ サービスを示したものです。これは Web 認証として同じ 設定です:

```
Router#show running-config
<output truncated>
 ! ! Set up the aaa new model to use the authentication proxy. ! aaa authorization auth-proxy
default group ! ! Apply a name to the authentication proxy configuration rule. ! ip admission
name example_auth_proxy_name proxy http inactivity-time 60 ! ! Apply the authentication proxy
rule at an interface. ! interface FastEthernet0/1 ip admission example_auth_proxy_name !
<output truncated>
```

次の例は同意ルール名前 example_consent_rule の下で同意機能で設定されるデバイスを識別したものです:

```
Router#show running-config
<output truncated>
 ! ! Apply a name to the consent configuration rule. ! ip admission name example_consent_rule
consent ! ! Apply the consent rule at an interface. ! interface FastEthernet 0/0 ip admission
consent-rule_rule ! <output truncated>
```

脆弱性を含んでいないことが確認された製品

以下の製品または機能はこの脆弱性の影響を受けません:

- Cisco IOS XR ソフトウェア
- Cisco IOS XE ソフトウェア
- FTP および Telnetセッションのためのファイアウォール認証プロキシ
- HTTP または同意機能のための認証プロキシで設定されない Cisco IOSデバイス

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 Firewall 認証プロキシ 機能はネットワーク管理者がユーザー単位の特定のセキュリティポリシーを適用することを可能にします。 認証プロキシ 機能を使うと、ユーザはネットワークにログインまたはインターネットに HTTP によってアクセスするためにでき、特定のアクセス プロファイルは CiscoSecure ACS、か他の RADIUS または TACACS+ 認証 サーバから自動的に取得され、適用されます。 そのユーザ プロファイルは、認証済みユーザからのアクティブなトラフィックが存在する間だけ有効です。 Web 認証機能は根本的な認証プロキシ 機能を利用しています。

Cisco IOS ルータのための同意機能は配線されるによってエンドユーザおよび同意 Web ページを示すことによって無線ネットワークに一時インターネットおよび法人アクセスを提供することを組織が可能にします。 同意機能はユーザ名 および パスワードの要求の有無にかかわらず使用することができますがまだ根本的な認証プロキシ 機能を利用しています。

認証プロキシによって認証されるこの脆弱性はセッションが第 1 なしで許可されるかまたは最初に同意 Web ページを確認しないで許可されるようにします。 少なくとも 1 人の正常に認証 された セッションか受け入れられた同意セッションは露出されるべき脆弱性のために存在 する必要があります。 これが発生する場合、RADIUS または TACACS+ サーバは、すべて最初 の 接続として同じ ユーザ名と認証されるようにパスワードが正しかったかどうかに関係なく AAAサーバで定義された、示しかどうか認証を、ユーザがおよび提供した認証情報に関係なく行っている場合後続のユーザーを。

この脆弱性はコードで競合状態、および悪意のあるユーザの制御の外部の複数の条件によってこの脆弱性が不正利用できる前に引き起こされ、会う必要があります。

HTTP のための認証プロキシのさらに詳しい詳細については次のリンクで Cisco IOS セキュリティ コンフィギュレーション ガイドを、リリース 12.4"認証の構成プロキシ」参照して下さい:
http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_cfg_authen_prxy_external_docbase_0900e4b1805afd05_4container_external_docbase_0900e4b1807b01d5.html

HTTPS のための認証プロキシのさらに詳しい詳細については次のリンクで Cisco IOS セキュリティ コンフィギュレーション ガイドを、リリース 12.4" HTTPS 認証プロキシのファイアウォール サポート」参照して下さい:
http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_fwall_https_prxy_external_docbase_0900e4b1805afe18_4container_external_docbase_0900e4b1807b01d5.html

同意機能のさらに詳しい詳細については次のリンクでユーザサービスを、リリース 12.2SR 「Cisco IOS ルータのための同意機能」保護する Cisco IOS セキュリティ コンフィギュレーション ガイドを参照して下さい:
http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cons_feat_rtrs_ps6922_TSD_Products_Configuration_Guide_Chapter.html

Web 認証機能のさらに詳しい詳細についてはソフトウェア コンフィギュレーション ガイドを、次のリンクで IEEE 802.1x ポートベース 認証」を設定するリリース 12.2(50)SE 「Catalyst 3750 シリーズスイッチ参照して下さい:
http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_50_se/configuration/guide/sw8021x.html#wp1401291

この脆弱性は次の Cisco バグ ID で文書化されています: **CSCsy15227** （登録ユーザのみ）およびよくある脆弱性および公開（CVE）識別子 CVE-2009-2863 は割り当てられました。

回避策

この脆弱性に対する回避策はありません。

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すべての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**
12.0	脆弱性なし	
12.0DA	脆弱性なし	
12.0DB	12.0(4)DB 以前のリリースは脆弱ではないです。 リリース 12.0(7)DB およびそれ以降は脆弱ではないです; first fixed in 12.4	12.4(23b) 12.4(25b)
12.0DC	12.0(3)DC1 以前のリリースは脆弱ではないです。 リリース 12.0(7)DC およびそれ以降は脆弱ではないです; first fixed in 12.4	12.4(23b) 12.4(25b)
12.0S	脆弱性なし	
12.0SC	脆弱性なし	
12.0SL	脆弱性なし	
12.0SP	脆弱性なし	
12.0ST	脆弱性なし	
12.0SX	脆弱性なし	
12.0SY	脆弱性なし	
12.0SZ	脆弱性なし	
12.0T	脆弱性あり; first fixed in 12.4	12.4(23b)

	12.0(4)T1 以前のリリースは脆弱ではないです。	12.4(25b)
12.0W	脆弱性なし	
12.0WC	12.0(5)WC4 以前のリリースは脆弱、リリース 12.0(5)WC4 およびそれ以降ではないです脆弱です	
12.0WT	脆弱性なし	
12.0XA	脆弱性なし	
12.0XB	脆弱性なし	
12.0XC	脆弱性なし	
12.0XD	脆弱性なし	
12.0XE	脆弱性あり; first fixed in 12.4 12.0(5)XE 以前のリリースは脆弱ではないです。	12.4(23b) 12.4(25b)
12.0XF	脆弱性なし	
12.0XG	脆弱性なし	
12.0XH	脆弱性なし	
12.0XI	脆弱性なし	
12.0XJ	脆弱性なし	
12.0XK	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.0XL	脆弱性なし	
12.0XM	脆弱性なし	
12.0XN	脆弱性なし	
12.0XQ	脆弱性なし	
12.0XR	脆弱性あり; first fixed in 12.4 12.0(6)XR 以前のリリースは脆弱ではないです。	12.4(23b) 12.4(25b)
12.0XS	脆弱性なし	
12.0XT	脆弱性なし	
12.0XV	脆弱性なし	
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(23b) 12.4(25b)
12.1AA	脆弱性なし	
12.1AX	脆弱性なし	
12.1AY	12.1(13)AY 以前のリリースは脆弱ではないです。 リリース 12.1(22)AY1 およびそれ以降は脆弱ではないです; first fixed in 12.2SE	12.2(50)SE3 12.2(52)SE; 13-OCT-2009 で利用可能

12.1AZ	脆弱性なし	
12.1CX	脆弱性なし	
12.1DA	脆弱性なし	
12.1DB	12.1(3)DB1 以前のリリースは脆弱ではないです。 リリース 12.1(4)DB1 およびそれ以降は脆弱ではないです; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1DC	12.1(4)DC 以前のリリースは脆弱ではないです。 リリース 12.1(4)DC2 およびそれ以降は脆弱ではないです; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1E	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	
12.1EA	12.1(6)EA1a 以前のリリースは脆弱ではないです。 リリース 12.1(8)EA1c およびそれ以降は脆弱ではないです; first fixed in 12.2SE	12.2(50)SE3; 13-OCT-2009 で利用可能
12.1EB	脆弱性なし	
12.1EC	脆弱性なし	
12.1EO	脆弱性なし	
12.1EU	脆弱性なし	
12.1EV	脆弱性なし	
12.1EW	脆弱性なし	
12.1EX	脆弱性あり; first fixed in 12.4 12.1(2)EX 以前のリリースは脆弱ではないです。	12.4(23b) 12.4(25b)
12.1EY	脆弱性なし	
12.1EZ	脆弱性なし	
12.1GA	脆弱性なし	
12.1GB	脆弱性なし	
12.1T	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XA	脆弱性なし	
12.1XB	脆弱性なし	
12.1XC	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XD	脆弱性なし	
12.1XE	脆弱性なし	
12.1XF	脆弱性なし	
12.1XG	脆弱性なし	
12.1XH	脆弱性あり; first fixed in 12.4	12.4(23b)

		12.4(25b)
12.1XI	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XJ	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XL	Release prior to 12.1(3a)XL2 are vulnerable， releases 12.1(3a)XL2 and later are not vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XM	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XP	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XQ	脆弱性なし	
12.1XR	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XS	脆弱性なし	
12.1XT	脆弱性あり; first fixed in 12.4 12.1(2)XT2 以前のリリースは脆弱ではないです。	12.4(23b) 12.4(25b)
12.1XU	脆弱性なし	
12.1XV	脆弱性なし	
12.1XW	脆弱性なし	
12.1XX	脆弱性なし	
12.1XY	脆弱性なし	
12.1XZ	脆弱性なし	
12.1YA	脆弱性なし	
12.1YB	脆弱性あり; first fixed in 12.4 12.1(5)YB 以前のリリースは脆弱ではないです。	12.4(23b) 12.4(25b)
12.1YC	脆弱性なし	
12.1YD	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
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(23b) 12.4(25b)
12.1YF	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1YH	脆弱性なし	
12.1YI	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	
12.1YJ	脆弱性なし	
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	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2B	脆弱性あり; first fixed in 12.4 12.2(2)B7 以前のリリースは脆弱ではないです。	12.4(23b) 12.4(25b)
12.2BC	脆弱性なし	
12.2BW	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
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	脆弱性あり; migrate to any release in 12.2SB	12.2(31)SB16 12.2(33)SB7
12.2DA	脆弱性なし	
12.2DD	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
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; first fixed in 12.2SE 12.2(37)EX 以前のリリースは脆弱ではないです。	12.2(50)SE3 12.2(52)SE; 13-OCT-2009 で利用可能
12.2EY	脆弱性あり; first fixed in 12.2SE 12.2(25)EY4 以前のリリースは脆弱ではないです。	12.2(50)SE3 12.2(52)SE; 13-OCT-2009 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	脆弱性あり; first fixed in 12.2SE	12.2(50)SE3 12.2(52)SE; 13-OCT-2009 で利用可能

12.2IRA	脆弱性あり; first fixed in 12.2SRD	12.2(33)SRD3
12.2IRB	脆弱性あり; first fixed in 12.2SRD	12.2(33)SRD3
12.2IRC	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	
12.2IXA	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	
12.2IXB	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	
12.2IXC	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	
12.2IXD	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	
12.2IXE	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	
12.2IXF	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	
12.2IXG	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	
12.2IXH	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	
12.2JA	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	注： Release prior to 12.2(30)S are vulnerable， releases 12.2(30)S and later are not vulnerable;	12.2(31)SB16 12.2(33)SB7
12.2SB	脆弱性なし	

12.2SBC	注： Release prior to 12.2(27)SBC3 are vulnerable，releases 12.2(27)SBC3 and later are not vulnerable;	12.2(31)SB16 12.2(33)SB7
12.2SCA	脆弱性なし	
12.2SCB	脆弱性なし	
12.2SE	12.2(50)SE3 12.2(52)SE; 13-OCT-2009 で利用可能	12.2(50)SE3 12.2(52)SE; 13-OCT-2009 で利用可能
12.2SEA	脆弱性なし	
12.2SEB	脆弱性なし	
12.2SEC	脆弱性あり; first fixed in 12.2SE	12.2(50)SE3 12.2(52)SE; 13-OCT-2009 で利用可能
12.2SED	脆弱性あり; first fixed in 12.2SE	12.2(50)SE3 12.2(52)SE; 13-OCT-2009 で利用可能
12.2SEE	脆弱性あり; first fixed in 12.2SE	12.2(50)SE3 12.2(52)SE; 13-OCT-2009 で利用可能
12.2SEF	Release prior to 12.2(25)SEF2 are vulnerable， releases 12.2(25)SEF2 and later are not vulnerable; first fixed in 12.2SE	12.2(50)SE3 12.2(52)SE; 13-OCT-2009 で利用可能
12.2SEG	Release prior to 12.2(25)SEG4 are vulnerable， releases 12.2(25)SEG4 and later are not vulnerable; first fixed in 12.2SE	12.2(50)SE3 12.2(52)SE; 13-OCT-2009 で利用可能
12.2SG	12.2(50)SG4 12.2(53)SG1; 07-DEC-2009 で利	12.2(50)SG4

	用可能	
12.2SGA	12.2(31)SGA11; 04-DEC-2009 で利用可能	12.2(31)SGA11; 04-DEC-2009 で利用可能
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; 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	
12.2SRA	脆弱性あり; first fixed in 12.2SRD	12.2(33)SRD3
12.2SRB	脆弱性あり; first fixed in 12.2SRD	12.2(33)SRD3
12.2SRC	12.2(33)SRC5; 29-OCT-2009 で利用可能	12.2(33)SRD3
12.2SRD	12.2(33)SRD2a 12.2(33)SRD3	12.2(33)SRD3
12.2STE	脆弱性なし	
12.2SU	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
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	
12.2SXA	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	
12.2SXB	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	
12.2SXD	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	
12.2SXE	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	
12.2SXF	12.2(18)SXF17; 30-SEP-2009 で利用可能 IOS software モジュール性パッチを参照して下さい	12.2(18)SXF17; 30-SEP-2009 で利用可能
12.2SXH	12.2(33)SXH6; 30-OCT-2009 で利用可能 IOS software モジュール性パッチを参照して下さい	12.2(33)SXH6; 30-OCT-2009 で利用可能
12.2SXI	12.2(33)SXI2 12.2(33)SXI2a	12.2(33)SXI2a
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(23b) 12.4(25b)
12.2TPC	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	
12.2XA	脆弱性あり; first fixed in 12.4 12.2(1)XA 以前のリリースは脆弱ではないです。	12.4(23b) 12.4(25b)
12.2XB	脆弱性あり; first fixed in 12.4 12.2(2)XB1 以前のリリースは脆弱ではないです。	12.4(23b) 12.4(25b)
12.2XC	脆弱性なし	
12.2XD	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XE	脆弱性なし	
12.2XF	脆弱性なし	
12.2XG	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XH	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XI	脆弱性なし	
12.2XJ	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XK	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XL	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XM	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)

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	脆弱性あり; first fixed in 12.2SG	12.2(31)SGA11 12.2(50)SG4
12.2XQ	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
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(23b) 12.4(25b)
12.2XU	脆弱性なし	
12.2XV	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XW	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2YA	Release prior to 12.2(4)YA8 are vulnerable ， releases 12.2(4)YA8 and later are not vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2YB	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	
12.2YC	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	
12.2YD	脆弱性なし	
12.2YE	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	
12.2YF	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	
12.2YG	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(23b) 12.4(25b)
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	
12.2YP	脆弱性なし	
12.2YQ	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	
12.2YR	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	
12.2YS	脆弱性なし	
12.2YT	脆弱性なし	
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	
12.2YY	脆弱性なし	
12.2YZ	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	

12.2ZA	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(23b) 12.4(25b)
12.2ZF	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2ZG	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2ZH	Release prior to 12.2(13)ZH6 are vulnerable ， releases 12.2(13)ZH6 and later are not vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
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	脆弱性なし	
12.2ZU	脆弱性あり; first fixed in 12.2SXH	12.2(33)SXH6; 30-OCT-2009 で利用可能
12.2ZX	脆弱性なし	
12.2ZY	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	
12.2ZYA	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	
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(23b) 12.4(25b)
12.3B	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)

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(23b) 12.4(25b)
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(23b) 12.4(25b)
12.3TPC	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	
12.3VA	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	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3XB	脆弱性なし	
12.3XC	Release prior to 12.3(2)XC4 are vulnerable ， releases 12.3(2)XC4 and later are not vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3XD	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3XE	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
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(23b) 12.4(25b)
12.3XI	脆弱性なし	
12.3XJ	脆弱性なし	

12.3XK	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3XL	脆弱性あり; first fixed in 12.4T	12.4(20)T4 12.4(22)T3 12.4(24)T2 ; 23-OCT-2009 で利用可能
12.3XQ	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3XR	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3XS	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3XU	脆弱性なし	
12.3XW	脆弱性なし	
12.3XX	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3XY	脆弱性なし	
12.3XZ	脆弱性なし	
12.3YA	脆弱性あり; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3YD	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
12.3YF	脆弱性なし	
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
12.3YI	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
12.3YJ	脆弱性なし	
12.3YK	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
12.3YM	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	脆弱性なし	
12.3YS	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
12.3YT	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	脆弱性なし	
12.3YX	脆弱性なし	
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(23a) 12.4(25a)	12.4(23b) 12.4(25b)
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)MR1 以前のリリースは脆弱、リリース 12.4(19)MR1 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(24)T1 12.4(20)T3 12.4(22)T2 12.4(15)T9	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	脆弱性なし	
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
12.4XG	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

12.4XL	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	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)T10 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	

Cisco IOSソフトウェア モジュール性-メンテナンス パック

Cisco IOS Software Modularity をご使用のお客様は、個別のメンテナンス パックを適用できます。 Cisco IOS Software Modularity についての追加情報は以下のリンクをご参照下さい: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_bulletin0900aecd80313e15.html

下記に記載されているメンテナンス パックは http://www.cisco.com/go/pn でダウンロードすることができます

12.2SXF のための Cisco IOSソフトウェア モジュール性メンテナンス パック

Cisco IOS ソフトウェア リリース	ソリューション メンテナンス Pack (MP)
12.2(18)SXF14	MP001
12.2(18)SXF15	MP001
12.2(18)SXF16	MP001

12.2SXH のための Cisco IOSソフトウェア モジュール性メンテナンス パック

Cisco IOS ソフトウェア リリース	ソリューション メンテナンス Pack (MP)
12.2(33)SXH5	MP001

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、Cisco の社内テストで発見されたものです。 Cisco PSIRT はインフラストラクチャの内で引き起こされるこの脆弱性を見た何人かの顧客に気づいているが、この脆弱性の悪質な宣伝に気づいていません。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-auth-proxy

改訂履歴

リビジョン 1.1	2009-October-19	更新済イオン ソフトウェア テーブル。
リビジョン 1.0	2009-September-23	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。