

Cisco IOSソフトウェア認証プロキシの脆弱性



アドバイザーID : cisco-sa-20090923-[CVE-2009-2863](#)
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](#)

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(S)、Web認証、または承諾機能の認証プロキシが設定されたCisco IOS®ソフトウェアには、認証されていないセッションが認証プロキシサーバをバイパスしたり、同意Webページをバイパスしたりすることを可能にする脆弱性が存在します。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。

この脆弱性を軽減する回避策はありません。

このアドバイザーは、<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-auth-proxy> で公開されています。

注 : 2009年9月23日のCisco IOSセキュリティアドバイザーバンドル公開には11件のSecurity Advisoryが含まれています。10件のアドバイザーは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。各アドバイザーには、そのアドバイザー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。

個々の公開リンクは、次のリンクの「Cisco Event Response: Semiannual Cisco IOS Software Advisory Bundled Publication」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

該当するバージョンのCisco IOSソフトウェアが稼働し、HTTP(S)、Web認証、または承諾機能の認証プロキシが設定されているデバイスには、脆弱性が存在します。

シスコ製品で稼働している Cisco IOS ソフトウェア リリースを確認するには、デバイスにログインして show version コマンドを使って、システム バナーを表示します。"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 ソフトウェア 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) が稼働し、そのイメージ名が C2500-IS-Lであることを示しています:

```
<#root>
```

```
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 ©) 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 が稼働し、そのイメージ名が C1841-ADVENTERPRISEK9-Mであることを示しています:

```
<#root>
```

```
Router#
```

```
show version
```

```
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version 12.4(20)T, RELEASE SOFTWARE (fc2)  
Technical Support: http://www.cisco.com/techsupport  
Copyright ©) 1986-2008 by Cisco Systems, Inc.  
Compiled Thu 10-Jul-08 20:25 by prod_rel_team
```

```
<output truncated>
```

Cisco IOSソフトウェアリリースの命名規則の追加情報は、次のリンクの「White Paper: Cisco IOS Reference Guide」で確認できます。 <http://www.cisco.com/warp/public/620/1.html>。

ご使用のデバイスで、HTTP(S)認証プロキシ、Web認証、または承諾機能のいずれかが設定されているかどうかを確認するには、デバイスにログインしてshow running-configコマンドを発行します。

次の例は、プロキシルール名example_auth_proxy_nameの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特定します。

```
<#root>

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>
```

次の例では、ip admissionコマンドを使用して、プロキシルール名example_auth_proxy_nameでHTTPに対して実行されているファイアウォール認証プロキシサービスを特定します。これは、Web認証と同じ設定です。

```
<#root>

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example_consent_ruleで承諾機能が設定されているデバイスを示しています。

```
<#root>  
  
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セッション用のファイアウォール認証プロキシ
- HTTP(S)認証プロキシまたは承諾機能が設定されていない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認証プロキシ機能を使用すると、ネットワーク管理者はユーザごとに特定のセキュリティポリシーを適用できます。認証プロキシ機能を使用すると、ユーザはネットワークにログインしたり、HTTP経由でインターネットにアクセスしたりでき、ユーザの特定のアクセスプロファイルがCiscoSecure ACSや他のRADIUSまたはTACACS+認証サーバから自動的に取得されて適用されます。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、基盤となる認証プロキシ機能を利用します。

Cisco IOSルータの承諾機能では、承諾用のWebページを表示することで、組織はエンドユーザに対して、エンドユーザの有線ネットワークおよびワイヤレスネットワークを介した一時的なインターネットアクセスおよび企業アクセスを提供できます。承諾機能は、ユーザ名とパスワードを要求する場合と要求しない場合の両方に使用できますが、基盤となる認証プロキシ機能は引き続き利用します。

この脆弱性を悪用すると、認証プロキシによって最初に認証されずにセッションが許可されるか、最初に同意Webページの確認応答を行わずにセッションが許可されます。脆弱性が公開されるには、認証に成功したセッションまたは承認された同意セッションが少なくとも1つ存在する必要があります。これが発生すると、RADIUSまたはTACACS+サーバでは、ユーザから提供された認証情報とAAAサーバで定義されているかどうか、およびパスワードが正しいかどうかに関係なく、認証を実行している場合は最初の接続と同じユーザ名を持つ後続のユーザが認証済みとして表示されます。

この脆弱性は、コード内の競合状態と、悪意のあるユーザの制御外のいくつかの状態によって引き起こされ、この脆弱性を不正利用する前に満たす必要があります。

HTTP認証プロキシの詳細については、次のリンクにある『Cisco IOS Security Configuration Guide, Release 12.4』の「Configuring Authentication Proxy」を参照してください。http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_cfg_authn_prxy_external_docbase_0900e4b1805afd05_4container_external_docbase_0900e4b1807b01d5.html

HTTPS認証プロキシの詳細については、次のリンクにある『Cisco IOS Security Configuration Guide, Release 12.4』の「Firewall Support of HTTPS Authentication Proxy」を参照してください。http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_fwll_https_prxy_external_docbase_0900e4b1805afe18_4container_external_docbase_0900e4b1807b01d5.html

承諾機能の詳細については、次のリンクにある『Cisco IOS Security Configuration Guide, Securing User Services, Release 12.2SR』の「Consent Feature for Cisco IOS Routers」を参照してください。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認証機能の詳細については、次のリンクにある『Catalyst 3750 Switch Software

Configuration Guide, Release 12.2(50)SE』の「Configuring IEEE 802.1x Port-Based Authentication」を参照してください。 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、Cisco Bug ID [CSCsy15227](#) (登録ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2009-2863が割り当てられています。

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

アップグレードを検討する場合は、<http://www.cisco.com/go/psirt> と後続のアドバイザリも参照して、問題の解決状況と完全なアップグレードソリューションを確認してください。

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わせください。

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。「Recommended Release」列は、このアドバイザリの公開時点で公開済みであるすべての脆弱性に対する修正を含むリリースを示します。特定の列に記載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も古い) 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	<p>12.0(4)DBまでのリリースには脆弱性はありません。</p> <p>リリース12.0(7)DB以降には脆弱性はありません。最初の修正は12.4です。</p>	<p>12.4(23b)</p> <p>12.4(25b)</p>
12.0DC	<p>12.0(3)DC1までのリリースには脆弱性はありません。</p> <p>リリース12.0(7)DC以降には脆弱性はありません。最初の修正は12.4です。</p>	<p>12.4(23b)</p> <p>12.4(25b)</p>
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(最初の修正は 12.4) 12.0(4)T1までのリリースには脆弱性はありません。	12.4(23b) 12.4(25b)
12.0W	脆弱性なし	
12.0WC	12.0(5)WC4より前のリリースには脆弱性があり、12.0(5)WC4以降のリリースには脆弱性はありません	
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(最初の修正は 12.4) 12.0(5)XEまでのリリースには脆弱性はありません。	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(最初の修正は 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(最初の修正は 12.4) 12.0(6)XRまでのリリースには脆弱性はありません。	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(最初の修正は 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までのリリースには脆弱性はありません。 リリース12.1(22)AY1以降には脆弱性はありません。最初の修正は 12.2SE です。	12.2(50)SE3 12.2(52)SE (2009年10月13日に入手可能)
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までのリリースには脆弱性はありません。 リリース12.1(4)DB1以降	12.4(23b) 12.4(25b)

	には脆弱性はありません。 最初の修正は 12.4 です。 。	
12.1DC	12.1(4)DCまでのリリースには脆弱性はありません。 リリース12.1(4)DC2以降には脆弱性はありません。 最初の修正は 12.4 です。 。	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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
12.1EA	12.1(6)EA1aまでのリリースには脆弱性はありません。 リリース12.1(8)EA1c以降には脆弱性はありません。最初の修正は 12.2SE です。	12.2(50)SE3 (2009年10月13日に入手可能)
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(最初の修正は 12.4) 12.1(2)EXまでのリリースには脆弱性はありません。	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(最初の修正は 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(最初の修正は 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(最初の修正は 12.4)	12.4(23b) 12.4(25b)
12.1XI	脆弱性あり(最初の修正は 12.4)	12.4(23b) 12.4(25b)
12.1XJ	脆弱性あり(最初の修正は 12.4)	12.4(23b) 12.4(25b)
12.1XL	12.1(3a)XL2より前のリリースには脆弱性があり、12.1(3a)XL2以降のリリースには脆弱性はありません。最初の修正は 12.4 です。	12.4(23b) 12.4(25b)
12.1XM	脆弱性あり(最初の修正は 12.4)	12.4(23b) 12.4(25b)
12.1XP	脆弱性あり(最初の修正は 12.4)	12.4(23b) 12.4(25b)
12.1XQ	脆弱性なし	

12.1XR	脆弱性あり(最初の修正は 12.4)	12.4(23b) 12.4(25b)
12.1XS	脆弱性なし	
12.1XT	脆弱性あり(最初の修正は 12.4) 12.1(2)XT2までのリリースには脆弱性はありません。	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(最初の修正は 12.4) 12.1(5)YBまでのリリースには脆弱性はありません。	12.4(23b) 12.4(25b)

12.1YC	脆弱性なし	
12.1YD	脆弱性あり(最初の修正は 12.4)	12.4(23b) 12.4(25b)
12.1YE	12.1(5)YE6より前のリリースには脆弱性があり、12.1(5)YE6以降のリリースには脆弱性はありません。最初の修正は 12.4 です。	12.4(23b) 12.4(25b)
12.1YF	脆弱性あり(最初の修正は 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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
12.1YJ	脆弱性なし	
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(最初の修正は 12.4)	12.4(23b) 12.4(25b)

12.2B	脆弱性あり(最初の修正は 12.4) 12.2(2)B7までのリリースには脆弱性はありません。	12.4(23b) 12.4(25b)
12.2BC	脆弱性なし	
12.2BW	脆弱性あり(最初の修正は 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。12.2SBの任意のリリースに移行	12.2(31)SB16 12.2(33)SB7
12.2DA	脆弱性なし	
12.2DD	脆弱性あり(最初の修正は 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(最初の修正は 12.2SE) 12.2(37)EX までのリリースには脆弱性はありません。	12.2(50)SE3 12.2(52)SE (2009年10月13日に入手可能)
12.2EY	脆弱性あり(最初の修正は 12.2SE) 12.2(25)EY4までのリリースには脆弱性はありません。	12.2(50)SE3 12.2(52)SE (2009年10月13日に入手可能)
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(最初の修正は 12.2SE)	12.2(50)SE3 12.2(52)SE (2009年10月13日に入手可能)
12.2IRA	脆弱性あり(最初の修正は 12.2SRD)	12.2(33)SRD3
12.2IRB	脆弱性あり(最初の修正は 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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
12.2IXE	脆弱性あり。このアドバイザリの「 修正済みソフ	

	トウェアの取得 」セクションの手順に従って、サポート組織にお問い合わせください	
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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
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：12.2(30)Sより前の	12.2(31)SB16

	リリースには脆弱性があり、12.2(30)S以降のリリースには脆弱性はありません。	12.2(33)SB7
12.2SB	脆弱性なし	
12.2SBC	注：12.2(27)SBC3より前のリリースには脆弱性があり、12.2(27)SBC3以降のリリースには脆弱性はありません。	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 (2009年10月13日に入手可能)	12.2(50)SE3 12.2(52)SE (2009年10月13日に入手可能)
12.2SEA	脆弱性なし	
12.2SEB	脆弱性なし	
12.2SEC	脆弱性あり(最初の修正は 12.2SE)	12.2(50)SE3 12.2(52)SE (2009年10月13日に入手可能)
12.2SED	脆弱性あり(最初の修正は 12.2SE)	12.2(50)SE3 12.2(52)SE (2009年

		10月13日に入手可能)
12.2SEE	脆弱性あり(最初の修正は 12.2SE)	12.2(50)SE3 12.2(52)SE (2009年10月13日に入手可能)
12.2SEF	12.2(25)SEF2より前のリリースには脆弱性があり、12.2(25)SEF2以降のリリースには脆弱性はありません。最初の修正は 12.2SE です。	12.2(50)SE3 12.2(52)SE (2009年10月13日に入手可能)
12.2SEG	12.2(25)SEG4より前のリリースには脆弱性があり、12.2(25)SEG4以降のリリースには脆弱性はありません。最初の修正は 12.2SE	12.2(50)SE3 12.2(52)SE (2009年10月13日に入手可能)
12.2SG	12.2(50)SG4 12.2(53)SG1 (2009年12月7日に入手可能)	12.2(50)SG4
12.2SGA	12.2(31)SGA11 (2009年12月4日に入手可能)	12.2(31)SGA11 (2009年12月4日に入手可能)
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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
12.2SRA	脆弱性あり(最初の修正は 12.2SRD)	12.2(33)SRD3
12.2SRB	脆弱性あり(最初の修正は 12.2SRD)	12.2(33)SRD3
12.2SRC	12.2(33)SRC5 (2009年10月29日に入手可能)	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(最初の修正は 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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
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の取得 」セクションの手順に従って、サ	

	ポート組織にお問い合わせください	
12.2SXF	12.2(18)SXF17 (2009年9月30日に入手可能) 「 IOS Software Modularity Patch 」を参照してください。	12.2(18)SXF17 (2009年9月30日に入手可能)
12.2SXH	12.2(33)SXH6 (2009年10月30日に入手可能) 「 IOS Software Modularity Patch 」を参照してください。	12.2(33)SXH6 (2009年10月30日に入手可能)
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(最初の修正は 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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	

12.2XA	脆弱性あり(最初の修正は 12.4) 12.2(1)XAまでのリリースには脆弱性はありません。	12.4(23b) 12.4(25b)
12.2XB	脆弱性あり(最初の修正は 12.4) 12.2(2)XB1までのリリースには脆弱性はありません。	12.4(23b) 12.4(25b)
12.2XC	脆弱性なし	
12.2XD	脆弱性あり(最初の修正は 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(最初の修正は 12.4)	12.4(23b) 12.4(25b)
12.2XH	脆弱性あり(最初の修正は 12.4)	12.4(23b) 12.4(25b)
12.2XI	脆弱性なし	
12.2XJ	脆弱性あり(最初の修正は 12.4)	12.4(23b)

		12.4(25b)
12.2XK	脆弱性あり(最初の修正は 12.4)	12.4(23b) 12.4(25b)
12.2XL	脆弱性あり(最初の修正は 12.4)	12.4(23b) 12.4(25b)
12.2XM	脆弱性あり(最初の修正は 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(最初の修正は 12.2SG)	12.2(31)SGA11 12.2(50)SG4
12.2XQ	脆弱性あり(最初の修正は 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(最初の修正は 12.4)	12.4(23b) 12.4(25b)
12.2XU	脆弱性なし	
12.2XV	脆弱性あり(最初の修正は 12.4)	12.4(23b) 12.4(25b)
12.2XW	脆弱性あり(最初の修正は 12.4)	12.4(23b) 12.4(25b)
12.2YA	12.2(4)YA8より前のリリースには脆弱性があり、12.2(4)YA8以降のリリースには脆弱性はありません。最初の修正は 12.4 です。	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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
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の取得 」セクションの手順に従って、サ	

	ポート組織にお問い合わせください	
12.2YM	脆弱性あり(最初の修正は 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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	

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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
12.2YV	12.2(11)YV1より前のリリースには脆弱性があり、12.2(11)YV1以降のリリースには脆弱性はありません	
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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	

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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
12.2ZE	脆弱性あり(最初の修正は 12.4)	12.4(23b) 12.4(25b)
12.2ZF	脆弱性あり(最初の修正は 12.4)	12.4(23b) 12.4(25b)
12.2ZG	脆弱性あり(最初の修正は 12.4)	12.4(23b) 12.4(25b)
12.2ZH	12.2(13)ZH6より前のリリースには脆弱性があり、12.2(13)ZH6以降のリリースには脆弱性はありません。最初の修正は 12.4 です。	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の取得 」セクションの手順に従って、サ	

	ポート組織にお問い合わせください	
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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
12.2ZP	脆弱性なし	
12.2ZU	脆弱性あり(最初の修正は 12.2SXH)	12.2(33)SXH6 (2009年10月30日に入手可能)
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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
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(最初の修正は 12.4)	12.4(23b) 12.4(25b)
12.3B	脆弱性あり(最初の修正は 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 までのリリースには脆弱性はありません。 リリース12.3(8)JK1以降には脆弱性はありません。最初の修正は 12.4 です。	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(最初の修正は 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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
12.3VA	脆弱性あり(最初の修正は 12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2 (2009年10月23日に入手可能)
12.3XA	脆弱性あり(最初の修正は 12.4)	12.4(23b) 12.4(25b)
12.3XB	脆弱性なし	
12.3XC	12.3(2)XC4より前のリリースには脆弱性があり、12.3(2)XC4以降のリリースには脆弱性はありません。最初の修正は 12.4 です。	12.4(23b) 12.4(25b)
12.3XD	脆弱性あり(最初の修正は 12.4)	12.4(23b) 12.4(25b)
12.3XE	脆弱性あり(最初の修正	12.4(23b)

	は 12.4)	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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
12.3XG	脆弱性あり(最初の修正は 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(最初の修正は 12.4)	12.4(23b) 12.4(25b)
12.3XL	脆弱性あり(最初の修正は 12.4T)	12.4(20)T4 12.4(22)T3 12.4(24)T2 (2009年10月23日に入手可能)
12.3XQ	脆弱性あり(最初の修正は 12.4)	12.4(23b) 12.4(25b)
12.3XR	脆弱性あり(最初の修正は 12.4)	12.4(23b) 12.4(25b)

12.3XS	脆弱性あり(最初の修正は 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(最初の修正は 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(最初の修正は 12.4)	12.4(23b) 12.4(25b)
12.3YD	脆弱性あり(最初の修正は 12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2 (2009年 10月23日に入手可能)
12.3YF	脆弱性なし	
12.3YG	脆弱性あり(最初の修正は 12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3

		12.4(24)T2 (2009年 10月23日に入手可能)
12.3YH	脆弱性あり(最初の修正 は 12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2 (2009年 10月23日に入手可能)
12.3YI	脆弱性あり(最初の修正 は 12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2 (2009年 10月23日に入手可能)
12.3YJ	脆弱性なし	
12.3YK	脆弱性あり(最初の修正 は 12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2 (2009年 10月23日に入手可能)
12.3YM	脆弱性あり(最初の修正 は 12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2 (2009年 10月23日に入手可能)

12.3YQ	脆弱性なし	
12.3YS	脆弱性あり(最初の修正は 12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2 (2009年10月23日に入手可能)
12.3YT	脆弱性あり(最初の修正は 12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2 (2009年10月23日に入手可能)
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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
12.3ZA	脆弱性あり(最初の修正は 12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2 (2009年10月23日に入手可能)

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より前のリリースには脆弱性があり、12.4(19)MR1以降のリリースには脆弱性はありません	
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 (2009年10月23日に入手可能)
12.4XA	脆弱性あり(最初の修正は 12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2 (2009年10月23日に入手可能)
12.4XB	脆弱性なし	
12.4XC	脆弱性あり(最初の修正は 12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2 (2009年10月23日に入手可能)
12.4XD	脆弱性あり(最初の修正は 12.4T)	12.4(15)T10 12.4(20)T4

		12.4(22)T3 12.4(24)T2 (2009年 10月23日に入手可能)
12.4XE	脆弱性あり(最初の修正 は 12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2 (2009年 10月23日に入手可能)
12.4XF	脆弱性あり(最初の修正 は 12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2 (2009年 10月23日に入手可能)
12.4XG	脆弱性なし	
12.4XJ	脆弱性あり(最初の修正 は 12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2 (2009年 10月23日に入手可能)
12.4XK	脆弱性あり(最初の修正 は 12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2 (2009年

		10月23日に入手可能)
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(最初の修正は 12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2 (2009年 10月23日に入手可能)
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の取得 」セクションの手順に従って、サポート組織にお問い合わせください	
12.4XW	脆弱性あり(最初の修正は 12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3

		12.4(24)T2 (2009年 10月23日に入手可能)
12.4XY	脆弱性あり(最初の修正 は 12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2 (2009年 10月23日に入手可能)
12.4XZ	脆弱性あり(最初の修正 は 12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2 (2009年 10月23日に入手可能)
12.4YA	脆弱性あり(最初の修正 は 12.4T)	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2 (2009年 10月23日に入手可能)
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 Software Modularity – 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の詳細については、次のリンクを参照してください。http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_bulletin0900aec80313e15.html

下記のメンテナンスパックは、<http://www.cisco.com/go/pn>からダウンロードできます。

12.2SXF用Cisco IOS Software Modularity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パック(MP)
12.2(18)SXF14	MP001
12.2(18)SXF15	MP001
12.2(18)SXF16	MP001

12.2SXH用Cisco IOS Software Modularity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パック(MP)
12.2(33)SXH5	MP001

推奨事項

`$propertyAndFields.get("recommendations")`

不正利用事例と公式発表

Cisco PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例やその公表は確認しておりません。

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では、この脆弱性の悪意のあるエクスプロイトを確認していません。ただし、インフラストラクチャ内でトリガーされたこの脆弱性を確認したお客様もいらっしゃいます。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-auth-proxy>

改訂履歴

リビジョン 1.1	2009年10月 19日	IONソフトウェアの表を更新。
リビジョン 1.0	2009年9月 23日	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、単独の転載や意識を施した場合、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。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。