Cisco IOSソフトウェアのコマンド許可バイパス

アドバイザリーID : cisco-sa-20120328-pai CVE-2012-0384
初公開日 : 2012-03-28 16:00
バージョン 1.0 : Final
CVSSスコア : 9.0
回避策 : No Workarounds available
Cisco バグ ID : CSCtr91106

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ソフトウェアには、認証、許可、アカウンティング(AAA)許可が使用される際に、リモートアプリケーションまたはデバイスが許可レベルを超える可能性のある脆弱性が存在します。この脆弱性を不正利用するには、Cisco IOSデバイスでHTTPまたはHTTPSサーバが有効になっている必要があります。

Cisco IOSソフトウェアを実行していない製品には脆弱性は存在しません。

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リリースしています。

このアドバイザリで説明されている脆弱性の回避策として、HTTPサーバが無効になっている可能性があります。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

注：2012年3月28日のCisco IOSソフトウェアセキュリティアドバイザリバンドル公開には9件のCisco Security Advisoryが含まれています。各アドバイザリには、このアドバイザリで説明されている脆弱性を修正したCisco IOSソフトウェアリリースと、2012年3月のバンドル公開のすべての脆弱性を修正したCisco IOSソフトウェアリリースが記載されています。

個々の公開リンクは、次のリンクの「Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication」に掲載されています。

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

該当製品

脆弱性のある製品

12.2以降のCisco IOSソフトウェアリリースが稼働し、HTTPまたはHTTPSサーバが設定されているデバイスは、AAA認証が使用されている場合、この脆弱性の影響を受けます。
HTTPまたはHTTPサーバがHTTPまたはHTTPSサーバで設定されているかどうかを確認するには、show ip http server status | include statusコマンドを使用します。次の例は、HTTPSサーバが有効でHTTPサーバが無効になっているCisco IOSデバイスを示しています。

```
<#root>

Router>

show ip http server status | include status

 HTTP server status: Disabled
 HTTP secure server status: Enabled
```

AAA認証が使用されているかどうかを確認するには、管理者がデバイスにログインして show run | include aaa authorizationコマンドを特権EXECモードで使用します。次の例に示すように、 aaa authorization commandsを示すエントリがある場合は、AAA認可が設定されています。

```
<#root>

Router#

show run | include aaa authorization commands

 aaa authorization commands 0 default local group tacacs+
 aaa authorization commands 1 default group tacacs+
 aaa authorization commands 15 default local
```

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。

次の例は、シスコ製品がCisco IOSソフトウェアリリース15.0(1)M1を実行し、インストールさ

れているイメージ名がC3900-UNIVERSALK9-Mであることを示しています。

```
<#root>

Router>

show version

Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1, RELEASE SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_team



!--- output truncated
```

Cisco IOSソフトウェアのリリース命名規則の追加情報は、次のリンクの『White Paper: Cisco IOS and NX-OS Software Reference Guide』で確認できます。
http://www.cisco.com/web/about/security/intelligence/ios-ref.htmlを参照。

脆弱性を含んでいないことが確認された製品

Cisco IOSまたはIOS XEソフトウェアを実行していない場合、この脆弱性の影響を受けません。AAA認証を使用していないデバイス、またはHTTPまたはHTTPSサーバが設定されていないデバイスは、この脆弱性の影響を受けません。

Cisco IOS XRは、この脆弱性の影響を受けません。

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

Cisco IOSソフトウェアを使用すると、リモートアプリケーションで、HTTPまたはHTTPS接続を介してCisco IOSソフトウェアを実行しているデバイスを管理および監視できます。

Cisco IOSのコマンド許可がバイパスされ、認証されたリモートのHTTPまたはHTTPSセッションで、許可レベルが設定された任意のCisco IOSコマンドを実行できる可能性のある脆弱性が存在します。この脆弱性は、認証されていないアクセスを許可しません。この脆弱性を不正利用するには、有効なユーザ名とパスワードが必要です。また、この脆弱性では、特権レベルが設定されていないコマンドをユーザが実行することはできません。

HTTPサーバは、Catalyst 3700シリーズ、Catalyst 3750シリーズ、Catalyst 3550シリーズ、

Catalyst 3560シリーズ、およびCatalyst 2950シリーズのシスコスイッチのクラスタ構成では、デフォルトで有効になっています。

AAA許可の詳細については、
http://www.cisco.com/en/US/docs/ios/12_2t/secure/command/reference/sftauth.htmlを参照してください。

Cisco IOSソフトウェアリリース12.2以降のリリースには脆弱性が存在する可能性があります。詳細については、次のリリース表を参照してください。

この脆弱性は、Cisco Bug ID CSCtr91106(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-2012-0384が割り当てられています。

回避策

HTTPサーバとHTTPSサーバが不要な場合は、 no ip http serverコマンドと no ip http secure-serverコマンドを使用して無効にすることができます。

ただし、Webサービスが必要な場合は、12.3(14)T以降で、選択的HTTPおよびHTTPSサービスを有効または無効にできる機能が導入されています。WEB_EXECサービスは、デバイスを設定し、リモートクライアントからデバイスの現在の状態を取得する機能を提供します。

他のHTTPサービスをアクティブなままにしたまま、WEB_EXECサービスを無効にすることができます。インストールでWEB_EXECサービスを使用する必要がない場合は、次の手順を使用して無効にすることができます。

1. すべてのセッションモジュールのリストを確認します。

```
<#root>

Router#

show ip http server session-module

HTTP server application session modules:
Session module Name  Handle Status   Secure-status  Description
HTTP_IFS              1      Active   Active         HTTP based IOS File Server
HOME_PAGE             2      Active   Active         IOS Homepage Server
QDM                   3      Active   Active         QOS Device Manager Server
QDM_SA                4      Active   Active         QOS Device Manager Signed Applet Server
WEB_EXEC              5      Active   Active         HTTP based IOS EXEC Server
IXI                   6      Active   Active         IOS XML Infra Application Server
IDCONF                7      Active   Active         IDCONF HTTP(S) Server
XSM                   8      Active   Active         XML Session Manager
VDM                   9      Active   Active         VPN Device Manager Server
XML_Api               10     Active   Active         XML Api
ITS                   11     Active   Active         IOS Telephony Service
ITS_LOCDIR            12     Active   Active         ITS Local Directory Search
CME_SERVICE_URL       13     Active   Active         CME Service URL
CME_AUTH_SRV_LOGIN    14     Active   Active         CME Authentication Server
```

```
IPS_SDEE              15     Active   Active         IOS IPS SDEE Server
tti-petitioner        16     Active   Active         TTI Petitioner
```

2. 必要なセッションモジュールのリストを作成します。この例では、WEB_EXEC以外のすべてが対象になります。

```
<#root>

Router#

configuration terminal

Router(config)#

ip http session-module-list exclude_webexec


HTTP_IFS,HOME_PAGE,QDM,QDM_SA,IXI,IDCONF,XSM,VDM,XML_Api,
ITS,ITS_LOCDIR,CME_SERVICE_URL,CME_AUTH_SRV_LOGIN,IPS_SDEE,tti-petitioner
```

3. リモートクライアントからの着信HTTP要求に対応するHTTP/HTTPSアプリケーションを選択的に有効にします。

```
<#root>

Router(config)#

ip http active-session-modules exclude_webexec

Router(config)#

ip http secure-active-session-modules exclude_webexec

Router(config)#

exit
```

4. すべてのセッションモジュールのリストを確認し、WEB_EXECがアクティブでないことを確認します。

```
<#root>

Router#

show ip http server session-module

HTTP server application session modules:
Session module Name  Handle Status   Secure-status  Description
HTTP_IFS              1      Active   Active         HTTP based IOS File Server
HOME_PAGE             2      Active   Active         IOS Homepage Server
QDM                   3      Active   Active         QOS Device Manager Server
QDM_SA                4      Active   Active         QOS Device Manager Signed Applet Server
WEB_EXEC              5      Inactive Inactive       HTTP based IOS EXEC Server
IXI                   6      Active   Active         IOS XML Infra Application Server
IDCONF                7      Active   Active         IDCONF HTTP(S) Server
XSM                   8      Active   Active         XML Session Manager
```

```
VDM                   9      Active   Active         VPN Device Manager Server
XML_Api               10     Active   Active         XML Api
ITS                   11     Active   Active         IOS Telephony Service
ITS_LOCDIR            12     Active   Active         ITS Local Directory Search
CME_SERVICE_URL       13     Active   Active         CME Service URL
CME_AUTH_SRV_LOGIN    14     Active   Active         CME Authentication Server
IPS_SDEE              15     Active   Active         IOS IPS SDEE Server
tti-petitioner        16     Active   Active         TTI Petitioner
```

HTTPサーバまたはセキュアHTTPサーバを使用してアプリケーションを選択的に有効にする方法の詳細については、Cisco IOSネットワーク管理設定ガイド、リリース12.4Tを参照してください。 http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_http_app_enable.html

HTTPサーバとWEB_EXECサービスが必要な場合は、信頼できる送信元だけを許可するようにHTTPサーバにアクセスできるホストを制限することが推奨されます。アクセスリストをHTTPサーバに適用して、アクセスを許可するホストを制限できます。アクセスリストをHTTPサーバに適用するには、グローバルコンフィギュレーションモードで ip http access-class {access-list-number | access-list-name}を使用してIPアドレスを取得できます。

次の例は、信頼できるホストだけがCisco IOS HTTPサーバにアクセスできるようにするアクセスリストを示しています。

```
ip access-list standard 20
     permit 192.168.1.0 0.0.0.255
     remark "Above is a trusted subnet"
     remark "Add further trusted subnets or hosts below"



          ! (Note: all other access implicitly denied) ! (Apply the access-list to the http server



     ip http access-class 20
```

Cisco IOS HTTPサーバの設定の詳細については、「 Cisco Webブラウザユーザインターフェイスの使用」を参照してください。

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場合は、http://www.cisco.com/go/psirt の Cisco Security Advisories and Responses アーカイブや後続のアドバイザリを参照して、侵害を受ける可能性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デバイス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規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約して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

次のCisco IOSソフトウェアテーブルの各行は、Cisco IOSソフトウェアトレインに対応しています。特定のトレインに脆弱性が存在する場合、修正を含む最も古いリリースが「最初の修正済みリリース」列に表示されます。2012年3月のFirst Fixed Release for All Advisories Bundled Publication列には、Cisco IOSソフトウェアセキュリティアドバイザリバンドル公開で公開されたすべての脆弱性を修正する最初のリリースが記載されています。シスコでは、可能な限り最新のリリースにアップグレードすることを推奨しています。

Cisco IOS Software Checkerを使用すると、特定のCisco IOSソフトウェアリリースに対応するシスコセキュリティアドバイザリを検索できます。このツールは、Cisco Security(SIO)ポータル(https://sec.cloudapps.cisco.com/security/center/selectIOSVersion.x)で利用できます。

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）	2012年3月のCisco IOSソフトウェアセキュリティアドバイザリバンドル公開に含まれるすべてのアドバイザリに対する最初の修正リリース
該当する 12.0 ベースのリリースはありません。		
Affected 12.2-Based Releases	First Fixed Release（修正された最初のリリース）	2012年3月のCisco IOSソフトウェアセキュリティアドバイザリバンドル公開に含まれるすべてのアドバイザリに対する最初の修正リリース
12.2	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2B	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2BC	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2BW	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2BX	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SB

12.2BY	脆弱性なし	脆弱性あり。最初の修正はリリース 15.0M
12.2BZ	脆弱性なし	脆弱性あり。最初の修正はリリース 15.0M
12.2CX	脆弱性なし	脆弱性あり。最初の修正はリリース 15.0M
12.2CY	脆弱性なし	脆弱性あり。最初の修正はリリース 15.0M
12.2CZ	脆弱性なし	脆弱性あり。最初の修正はリリース 12.0S
12.2DA	脆弱性なし	脆弱性あり。最初の修正はリリース 15.0M
12.2DD	脆弱性なし	脆弱性あり。最初の修正はリリース 15.0M
12.2DX	脆弱性なし	脆弱性あり。最初の修正はリリース 15.0M
12.2EU	脆弱性なし	脆弱性が存在します。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。
12.2EW	脆弱性が存在します。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。 12.2(20)EWA4までのリリースには脆弱性はありません。	脆弱性が存在します。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。
12.2EWA	脆弱性が存在します。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。	脆弱性が存在します。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。

	12.2(20)EWA4までのリリースには脆弱性はありません。	
12.2EX	脆弱性あり。最初の修正はリリース15.0SE 12.2(25)EX1までのリリースには脆弱性はありません。	脆弱性あり。最初の修正はリリース15.0SE
12.2EY	12.2(52)EY4 12.2(58)EY2	12.2(52)EY4
12.2EZ	脆弱性あり。最初の修正はリリース15.0SE	脆弱性あり。最初の修正はリリース15.0SE
12.2FX	脆弱性あり。最初の修正はリリース12.2SE	脆弱性あり。最初の修正はリリース15.0SE
12.2FY	脆弱性あり。最初の修正はリリース15.0SE	脆弱性あり。最初の修正はリリース15.0SE
12.2FZ	脆弱性あり。最初の修正はリリース12.2SE	脆弱性あり。最初の修正はリリース15.0SE
12.2IRA	脆弱性あり。最初の修正はリリース12.2SRD	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRB	脆弱性あり。最初の修正はリリース12.2SRD	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRC	脆弱性あり。最初の修正はリリース12.2SRD	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRD	脆弱性あり。最初の修正はリリース12.2SRD	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRE	脆弱性あり。最初の修正はリリース12.2SRD	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRF	脆弱性あり。最初の修正はリリース12.2SRD	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRG	脆弱性が存在します。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。	脆弱性が存在します。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。

12.2IRH	12.2(33)IRH1	脆弱性が存在します。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	脆弱性なし	脆弱性が存在します。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	脆弱性なし	脆弱性が存在します。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	脆弱性なし	脆弱性が存在します。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	脆弱性なし	脆弱性が存在します。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	脆弱性なし	脆弱性が存在します。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	脆弱性なし	脆弱性が存在します。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	脆弱性なし	脆弱性が存在します。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	脆弱性なし	脆弱性が存在します。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	脆弱性なし
12.2JK	脆弱性なし	脆弱性なし
12.2MB	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2MC	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2MRA	脆弱性あり。最初の修正はリリース12.2SRD	脆弱性あり。最初の修正はリリース12.2SRE
12.2MRB	脆弱性が存在します。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。	脆弱性が存在します。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。
12.2S	脆弱性なし	12.2(30)Sより前の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。最初の修正はリリース12.0S
12.2SB	12.2(33)SB12	12.2(33)SB12
12.2SBC	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRE
12.2SCA	脆弱性あり。最初の修正はリリース12.2SCE	脆弱性あり。最初の修正はリリース12.2SCE
12.2SCB	脆弱性あり。最初の修正はリリース12.2SCE	脆弱性あり。最初の修正はリリース12.2SCE
12.2SCC	脆弱性あり。最初の修正はリリース12.2SCE	脆弱性あり。最初の修正はリリース12.2SCE
12.2SCD	脆弱性あり。最初の修正はリリース12.2SCE	脆弱性あり。最初の修正はリリース12.2SCE

12.2SCE	12.2(33)SCE5	12.2(33)SCE6
12.2SCF	12.2(33)SCF2	12.2(33)SCF2
12.2SE	12.2(55)SE5	12.2(55)SE5 *
12.2SEA	脆弱性あり。最初の修正はリリース12.2SE	脆弱性あり。最初の修正はリリース15.0SE
12.2SEB	脆弱性あり。最初の修正はリリース12.2SE	脆弱性あり。最初の修正はリリース15.0SE
12.2SEC	脆弱性あり。最初の修正はリリース12.2SE	脆弱性あり。最初の修正はリリース15.0SE
12.2SED	脆弱性あり。最初の修正はリリース12.2SE	脆弱性あり。最初の修正はリリース15.0SE
12.2SEE	脆弱性あり。最初の修正はリリース12.2SE	脆弱性あり。最初の修正はリリース15.0SE
12.2SEF	脆弱性あり。最初の修正はリリース12.2SE	脆弱性あり。最初の修正はリリース15.0SE
12.2SEG	脆弱性あり。最初の修正はリリース15.0SE	脆弱性あり。最初の修正はリリース15.0SE
12.2SG	12.2(53)SG7（2012年5月7日に入手可能）	12.2(53)SG7（2012年5月7日に入手可能）
12.2SGA	脆弱性あり。最初の修正はリリース12.2SG	脆弱性が存在します。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。
12.2SL	脆弱性なし	脆弱性なし
12.2SM	脆弱性なし	脆弱性が存在します。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。
12.2SO	脆弱性なし	脆弱性が存在します。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。

12.2SQ	脆弱性が存在します。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。	脆弱性が存在します。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。最初の修正はリリース12.2SRD	脆弱性あり。最初の修正はリリース12.2SRE
12.2SRB	脆弱性あり。最初の修正はリリース12.2SRD	脆弱性あり。最初の修正はリリース12.2SRE
12.2SRC	脆弱性あり。最初の修正はリリース12.2SRD	脆弱性あり。最初の修正はリリース12.2SRE
12.2SRD	12.2(33)SRD8	脆弱性あり。最初の修正はリリース12.2SRE
12.2SRE	12.2(33)SRE6	12.2(33)SRE6
12.2STE	脆弱性が存在します。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。	脆弱性が存在します。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。
12.2SU	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2SV	脆弱性なし	12.2(18)SV2 までのリリースには脆弱性はありません。
12.2SVA	脆弱性なし	脆弱性が存在します。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。
12.2SVC	脆弱性なし	脆弱性が存在します。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。
12.2SVD	脆弱性なし	脆弱性が存在します。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。
12.2SVE	脆弱性なし	脆弱性が存在します。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。
12.2SW	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.2SX	脆弱性なし	脆弱性が存在します。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	脆弱性なし	脆弱性が存在します。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	脆弱性なし	脆弱性が存在します。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	脆弱性なし	脆弱性が存在します。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	脆弱性なし	脆弱性が存在します。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	脆弱性なし	脆弱性が存在します。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。
12.2SXH	脆弱性が存在します。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。	脆弱性が存在します。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。
12.2SXI	12.2(33)SXI9	12.2(33)SXI9
12.2日本語	12.2(33)SXJ2	12.2(33)SXJ2
12.2SY	12.2(50)SY2（2012年6月11日に入手可能） 12.2(14)SY5までのリリースには脆弱性はありません。	12.2(50)SY2（2012年6月11日に入手可能）
12.2SZ	脆弱性なし	脆弱性あり。最初の修正はリリース12.0S
12.2T	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2TPC	脆弱性なし	脆弱性が存在します。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	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2XB	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2XC	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2XD	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2XE	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2XF	脆弱性なし	脆弱性あり。最初の修正はリリース

		15.0M
12.2XG	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2XH	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2XI	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2XJ	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2XK	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2XL	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2XM	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2XNA	Cisco IOS XE ソフトウェアの可用性を参照してください。	Cisco IOS XE ソフトウェアの可用性を参照してください。
12.2XNB	Cisco IOS XE ソフトウェアの可用性を参照してください。	Cisco IOS XE ソフトウェアの可用性を参照してください。
12.2XNC	Cisco IOS XE ソフトウェアの可用性を参照してください。	Cisco IOS XE ソフトウェアの可用性を参照してください。
12.2XND	Cisco IOS XE ソフトウェアの可用性を参照してください。	Cisco IOS XE ソフトウェアの可用性を参照してください。
12.2XNE	Cisco IOS XE ソフトウェアの可用性を参照してください。	Cisco IOS XE ソフトウェアの可用性を参照してください。
12.2XNF	Cisco IOS XE ソフトウェアの可用性を参照してください。	Cisco IOS XE ソフトウェアの可用性を参照してください。
12.2XO	脆弱性あり。最初の修正はリリース12.2SG	脆弱性が存在します。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

		。
12.2XQ	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2XR	脆弱性なし	12.2(15)XRより前のリリースには脆弱性があり、12.2(15)XR以降のリリースには脆弱性はありません。最初の修正はリリース15.0M
12.2XS	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2XT	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2XU	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2XV	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2XW	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2YA	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2YC	脆弱性なし	脆弱性が存在します。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	脆弱性が存在します。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。
12.2YE	脆弱性なし	脆弱性が存在します。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	脆弱性が存在します。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	脆弱性なし	脆弱性が存在します。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	脆弱性あり。最初の修正はリリース15.0M 12.2(8)YPまでのリリースには脆弱性はありません。
12.2YT	脆弱性なし	脆弱性が存在します。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。
12.2YW	脆弱性なし	脆弱性が存在します。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。
12.2YX	脆弱性なし	脆弱性が存在します。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	脆弱性が存在します。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。
12.2YZ	脆弱性なし	脆弱性が存在します。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	脆弱性が存在します。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。
12.2ZB	脆弱性なし	脆弱性が存在します。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。
12.2ZC	脆弱性なし	脆弱性が存在します。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。
12.2ZD	脆弱性なし	脆弱性が存在します。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	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M
12.2ZH	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.2ZJ	脆弱性なし	脆弱性が存在します。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	脆弱性が存在します。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。
12.2ZU	脆弱性なし	脆弱性が存在します。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。
12.2ZX	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRE

12.2ZY	脆弱性なし	脆弱性が存在します。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	脆弱性なし	脆弱性が存在します。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）	2012年3月のCisco IOSソフトウェアセキュリティアドバイザリバンドル公開に含まれるすべてのアドバイザリに対する最初の修正リリース
12.3	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3B	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3BC	脆弱性あり。最初の修正はリリース12.2SCE	脆弱性あり。最初の修正はリリース12.2SCE
12.3BW	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3JA	脆弱性あり。最初の修正はリリース12.4JA	脆弱性あり。最初の修正はリリース12.4JA
12.3JEA	脆弱性が存在します。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。	脆弱性が存在します。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。
12.3JEB	脆弱性が存在します。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。	脆弱性が存在します。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。

12.3JEC	脆弱性が存在します。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。	脆弱性が存在します。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。
12.3JED	脆弱性が存在します。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。	脆弱性が存在します。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。
12.3JK	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3JL	脆弱性が存在します。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。	脆弱性が存在します。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。
12.3JX	脆弱性なし	脆弱性なし
12.3T	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3TPC	脆弱性が存在します。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。	脆弱性が存在します。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	脆弱性なし	脆弱性なし
12.3XA	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3XB	脆弱性が存在します。このアドバイザリの「修正済みソフトウェア	脆弱性が存在します。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

	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。	ポート組織にお問い合わせください。
12.3XC	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3XD	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3XE	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3XF	脆弱性が存在します。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。	脆弱性が存在します。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。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3XI	脆弱性あり。最初の修正はリリース12.2SB	脆弱性あり。最初の修正はリリース12.2SRE
12.3XJ	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3XK	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3XL	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3XQ	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3XR	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3XU	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース12.4T
12.3XW	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3XX	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M

12.3XY	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3XZ	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M
12.3YD	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3YF	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3YG	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3YI	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3YJ	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3YK	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3YM	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3YQ	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3YS	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3YT	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3YU	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3YX	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.3YZ	脆弱性が存在します。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。	脆弱性が存在します。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	脆弱性あり。最初の修正はリリース

	正はリリース12.4T	15.0M
Affected 12.4-Based Releases	First Fixed Release（修正された最初のリリース）	2012年3月のCisco IOSソフトウェアセキュリティアドバイザリバンドル公開に含まれるすべてのアドバイザリに対する最初の修正リリース
12.4	12.4(25g)（2012年9月19日に入手可能）	脆弱性あり。最初の修正はリリース15.0M
12.4GC	脆弱性が存在します。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。	脆弱性が存在します。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。
12.4JA	12.4(23c)JA4 12.4(25d)JA2（2012年8月1日に入手可能） 12.4(25e)JA	12.4(23c)JA412.4(25e)JA
12.4JAX	脆弱性あり。最初の修正はリリース12.4JA	脆弱性あり。最初の修正はリリース12.4JA
12.4JDA	脆弱性が存在します。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。	脆弱性が存在します。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。
12.4JDC	脆弱性が存在します。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。	脆弱性が存在します。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。
12.4JDD	脆弱性が存在します。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	脆弱性が存在します。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。

	ト組織にお問い合わせください。	
12.4JDE	脆弱性が存在します。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。	脆弱性が存在します。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。
12.4JHA	脆弱性が存在します。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。	脆弱性が存在します。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。
12.4JHB	脆弱性が存在します。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。	脆弱性が存在します。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。
12.4JHC	脆弱性が存在します。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。	脆弱性が存在します。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。
12.4JK	脆弱性が存在します。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。	脆弱性が存在します。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。
12.4JL	脆弱性が存在します。このアドバイザリの「修正済みソフトウェア	脆弱性が存在します。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

	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。	ポート組織にお問い合わせください。
12.4JX	脆弱性あり。最初の修正はリリース12.4JA	脆弱性あり。最初の修正はリリース12.4JA
12.4JY	脆弱性あり。最初の修正はリリース12.4JA	脆弱性あり。最初の修正はリリース12.4JA
12.4JZ	脆弱性あり。最初の修正はリリース12.4JA	脆弱性あり。最初の修正はリリース12.4JA
12.4MD	12.4(22)MD3（2012年3月30日に入手可能）	12.4(22)MD3（2012年3月30日に入手可能）
12.4MDA	12.4(24)MDA11	12.4(24)MDA11
12.4MDB	12.4(24)MDB5a	12.4(24)MDB5a
12.4MDC	脆弱性なし	脆弱性なし
12.4MR	脆弱性が存在します。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。	脆弱性が存在します。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。
1240万	脆弱性が存在します。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。	脆弱性が存在します。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。
12.4MRB	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4SW	12.4(15)SW8a	脆弱性あり。最初の修正はリリース15.0M
12.4T	12.4(15)T17 12.4(24)T7	12.4(15)T17 12.4(24)T7
12.4XA	脆弱性あり。最初の修	脆弱性あり。最初の修正はリリース

	正はリリース12.4T	15.0M
12.4XB	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース12.4T
12.4XC	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4XD	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4XE	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4XF	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4XG	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4XJ	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4XK	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4XL	脆弱性が存在します。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。	脆弱性が存在します。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。
12.4XM	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4XN	脆弱性が存在します。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。	脆弱性が存在します。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。
12.4XP	脆弱性が存在します。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	脆弱性が存在します。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

	手順に従って、サポート組織にお問い合わせください。	。
12.4XQ	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4XR	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース12.4T
12.4XT	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4XV	脆弱性が存在します。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。	脆弱性が存在します。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。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4XY	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4XZ	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4YA	脆弱性あり。最初の修正はリリース12.4T	脆弱性あり。最初の修正はリリース15.0M
12.4YB	脆弱性が存在します。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。	脆弱性が存在します。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。
12.4YD	脆弱性が存在します。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。	脆弱性が存在します。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。

12.4YE	12.4(24)YE3d	12.4(24)YE3d
12.4YG	12.4(24)YG4	12.4(24)YG4
影響を受ける 15.0 ベースのリリース	First Fixed Release（修正された最初のリリース）	2012年3月のCisco IOSソフトウェアセキュリティアドバイザリバンドル公開に含まれるすべてのアドバイザリに対する最初の修正リリース
15.0M	15.0(1)M8	15.0(1)M8
15.0MR	脆弱性が存在します。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。	脆弱性が存在します。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。
15.0MRA	脆弱性が存在します。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。	脆弱性が存在します。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。
15.0秒	15.0(1)S5 Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。	15.0(1)S5 Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。
15.0SA	脆弱性なし	脆弱性なし
15.0SE	15.0(1)SE1 15.0(2)SE（2012年8月6日に入手可能）	15.0(1)SE1
15.0SG	15.0(2)SG2 Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。	15.0(2)SG2 Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。
15.0SY	15.0(1)SY1	15.0(1)SY1
15.0XA	脆弱性あり。最初の修正はリリース15.1T	脆弱性あり。最初の修正はリリース15.1T

15.0XO	脆弱性あり。最初の修正はリリース15.0SG Cisco IOS XEデバイスです。「Cisco IOS XEソフトウェアの可用性」を参照してください。	脆弱性あり。最初の修正はリリース15.0SG Cisco IOS XEデバイスです。「Cisco IOS XEソフトウェアの可用性」を参照してください。
影響を受ける 15.1 ベースのリリース	First Fixed Release（修正された最初のリリース）	2012年3月のCisco IOSソフトウェアセキュリティアドバイザリバンドル公開に含まれるすべてのアドバイザリに対する最初の修正リリース
15.1EY	15.1(2)EY1a	15.1(2)EY2
15.1GC	15.1(2)GC2	15.1(2)GC2
1,510万	15.1(4)M2	15.1(4)M4（2012年3月30日に入手可能）
15.1MR	15.1(1)MR3	脆弱性が存在します。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。
15.1S	15.1(3)S2 Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。	15.1(3)S2 Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。
15.1SG	脆弱性なし	脆弱性なし
15.1SNG	脆弱性が存在します。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。	脆弱性が存在します。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。
15.1SNH	脆弱性なし	脆弱性なし
15.1T	15.1(1)T4 15.1(2)T5（2012年4月27日に入手可能） 15.1(3)T3	15.1(3)T3

15.1XB	脆弱性あり。最初の修正はリリース15.1T	脆弱性あり。最初の修正はリリース15.1T
Affected 15.2-Based Releases	First Fixed Release（修正された最初のリリース）	2012年3月のCisco IOSソフトウェアセキュリティアドバイザリバンドル公開に含まれるすべてのアドバイザリに対する最初の修正リリース
15.2GC	15.2(1)GC1	15.2(1)GC2
15.2秒	15.2(1)S1 Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。	15.2(1)S1 Cisco IOS XEデバイス：「Cisco IOS XEソフトウェアの可用性」を参照してください。
15.2T	15.2(1)T1 15.2(2)T 15.2(2)T1	15.2(1)T215.2(2)T115.2(3)T（2012年3月30日に入手可能）

* Cisco Catalyst 3550シリーズスイッチは、インターネットキーエクスチェンジ(IKE)機能をサポートしており、デバイスでレイヤ3イメージを実行している場合はCisco Bug ID CSCts38429に対して脆弱です。ただし、この製品はソフトウェアメンテナンスが終了しています。 レイヤ2イメージを実行しているCisco 3550シリーズSMIスイッチはIKEをサポートしていないため、脆弱ではありません。 12.2SEベースのソフトウェアを実行する他のシスコデバイスには、この脆弱性は存在しません。

Cisco IOS XE ソフトウェア

Cisco IOS XEソフトウェアは、このアドバイザリで説明されている脆弱性の影響を受けます。

Cisco IOS XE ソフトウェア リリース	First Fixed Release（修正された最初のリリース）	2012年3月のCisco IOSソフトウェアセキュリティアドバイザリバンドル公開に含まれるすべてのアドバイザリに対する最初の修正リリース
2.1.x	脆弱性あり。3.1.2S以降に移行してください。	脆弱性あり。3.4.2S以降に移行してください。
2.2.x	脆弱性あり。3.1.2S以降に移	脆弱性あり。3.4.2S以降に移行してください。

	行してください。	
2.3.x	脆弱性あり。3.1.2S以降に移行してください。	脆弱性あり。3.4.2S以降に移行してください。
2.4.x	脆弱性あり。3.1.2S以降に移行してください。	脆弱性あり。3.4.2S以降に移行してください。
2.5.x	脆弱性あり。3.1.2S以降に移行してください。	脆弱性あり。3.4.2S以降に移行してください。
2.6.x	脆弱性あり。3.1.2S以降に移行してください。	脆弱性あり。3.4.2S以降に移行してください。
3.1.xS	3.1.2S	脆弱性あり。3.4.2S以降に移行してください。
3.1.xSG	脆弱性あり。3.2.2SG以降に移行してください。	脆弱性あり。3.2.2SG以降に移行してください。
3.2.xS	脆弱性あり。3.4.2S以降に移行してください。	脆弱性あり。3.4.2S以降に移行してください。
3.2.xSG	3.2.2SG	3.2.2SG
3.3.xS	脆弱性あり。3.4.2S以降に移行してください。	脆弱性あり。3.4.2S以降に移行してください。
3.2.xSG	脆弱性なし	脆弱性なし
3.4.xS	3.4.2S	3.4.2S
3.5.xS	3.5.1S	3.5.1S
3.6.xS	脆弱性なし	脆弱性なし

Cisco IOS ソフトウェア リリースへの Cisco IOS XE ソフトウェア リリースのマッピングについては、「Cisco IOS XE 2 Release Notes」、「Cisco IOS XE 3S Release Notes」、および「Cisco IOS XE 3SG Release Notes」を参照してください。

Cisco IOS XR ソフトウェア

Cisco IOS XRソフトウェアは、2012年3月のCisco IOS Software Security Advisoryバンドル公開に含まれている脆弱性の影響を受けません。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）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を確認していません。

この脆弱性は、デバイスの通常の動作中に脆弱性を観察したお客様からCisco TACに報告されたものです。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

改訂履歴

リビジョン 1.0	2012年3月28日	初版リリース

利用規約

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。