Cisco IOSソフトウェアのResource Reservation Protocolに関するDoS脆弱性

アドバイザリーID : cisco-sa-20130327-rsvp CVE-2013-1143
初公開日 : 2013-03-27 16:00
最終更新日 : 2013-04-11 15:00
バージョン 1.2 : Final
CVSSスコア : 7.1
回避策 : No Workarounds available
Cisco バグ ID : CSCtg39957

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ソフトウェアおよびCisco IOS XEソフトウェアのResource Reservation Protocol(RSVP)機能は、Multiprotocol Label Switching(MPLS-TE)が有効なデバイスで使用された場合に脆弱性が発生します。この脆弱性の不正利用に成功すると、認証されていないリモートの攻撃者によって該当デバイスのリロードが引き起こされる可能性があります。繰り返し不正利用されると、Denial of Service（DoS）状態が続く可能性があります。

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-20130327-rsvp

注：2013年3月27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7件のCisco Security Advisoryが含まれています。 すべてのアドバイザリは、Cisco IOSソフトウェアの脆弱性に対処しています。各Cisco IOSソフトウェアセキュリティアドバイザリには、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、2013年3月のバンドル公開のすべてのCisco IOSソフトウェア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: Semiannual 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_mar13.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ソフトウェアまたはCisco IOS XEソフトウェアを実行しているシスコデバイスは、MPLS-TEが有効に設定されている場合に脆弱性が存在します。
脆弱性のある設定には、次のグローバルコンフィギュレーションコマンドが含まれます。
<#root>

```
mpls traffic-eng tunnels
```

この脆弱性は、デバイス宛てのトラフィックによってのみ引き起こされます。通過トラフィックによって脆弱性が引き起こされることはありません。

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

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。Cisco IOS XRには脆弱性はありません。

詳細

Cisco IOSソフトウェアおよびCisco IOS XEソフトウェアのRSVP機能は、MPLS-TEが有効なデバイスで使用された場合に脆弱性が存在します。この脆弱性の不正利用に成功すると、認証されていないリモートの攻撃者によって該当デバイスのリロードが引き起こされる可能性があります。繰り返し不正利用されると、Denial of Service（DoS）状態が続く可能性があります。

この脆弱性は、正当でありながら一般的ではないトラフィックエンジニアリングPATHメッセージの不適切な処理によって引き起こされます。

この脆弱性は、Cisco Bug ID CSCtg39957(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2013-1143が割り当てられています

脆弱性のある設定には、次のグローバルコンフィギュレーションコマンドが含まれます。
<#root>

```
mpls traffic-eng tunnels
```

この脆弱性は、デバイス宛てのトラフィックによってのみ引き起こされます。通過トラフィックによって脆弱性が引き起こされることはありません。

回避策

この脆弱性を軽減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場合は、http://www.cisco.com/go/psirt のシスコ セキュリティ アドバイザリ、応答、および通知のアーカイブや、後続のアドバイザリを参照して侵害の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。2013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。可能な場合は、利用可能な最新のリリースにアップグレードすることをお勧めします。

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）	2013年3月の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）	2013年3月の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	脆弱性なし
12.2B	脆弱性なし	脆弱性なし
12.2BC	脆弱性なし	脆弱性なし
12.2BW	脆弱性なし	脆弱性なし
12.2BX	脆弱性なし	脆弱性なし
12.2BY	脆弱性なし	脆弱性なし
12.2BZ	脆弱性なし	脆弱性なし
12.2CX	脆弱性なし	脆弱性なし
12.2CY	脆弱性なし	脆弱性なし
12.2CZ	脆弱性なし	脆弱性なし
12.2DA	脆弱性なし	脆弱性なし
12.2DD	脆弱性なし	脆弱性なし
12.2DX	脆弱性なし	脆弱性なし
12.2EU	脆弱性なし	脆弱性なし
12.2EW	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SG

		12.2(20)EW4までのリリースには脆弱性はありません。
12.2EWA	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SG 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(55)EX3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 12.2(37)EX までのリリースには脆弱性はありません。
12.2EY	脆弱性なし	脆弱性あり。最初の修正はリリース15.2S
12.2EZ	脆弱性あり。最初の修正はリリース15.0SE 12.2(55)EZ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
12.2FX	脆弱性なし	脆弱性あり。最初の修正はリリース15.0SE
12.2FY	脆弱性なし	脆弱性あり。最初の修正はリリース15.0SE
12.2FZ	脆弱性なし	脆弱性あり。最初の修正はリリース15.0SE
12.2IRA	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRB	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRC	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRD	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRE	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRF	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRE
12.2IRG	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。
12.2IRH	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。
12.2IRI	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。
12.2IXA	脆弱性なし	脆弱性なし
12.2IXB	脆弱性なし	脆弱性なし
12.2IXC	脆弱性なし	脆弱性なし
12.2IXD	脆弱性なし	脆弱性なし
12.2IXE	脆弱性なし	脆弱性なし
12.2IXF	脆弱性なし	脆弱性なし
12.2IXG	脆弱性なし	脆弱性なし
12.2IXH	脆弱性なし	脆弱性なし
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	脆弱性なし
12.2MC	脆弱性なし	脆弱性なし
12.2MRA	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRE
12.2MRB	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。
12.2S	脆弱性なし	Vulnerable.脆弱性が存在するのは、リリース12.2(25)S ~ 12.2(25)S15だけです
12.2SB	脆弱性なし	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12.2SB
12.2SCA	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SCF
12.2SCB	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SCF
12.2SCC	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SCF
12.2SCD	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SCF

12.2SCE	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SCF
12.2SCF	脆弱性なし	12.2(33)SCF4
12.2SCG	脆弱性なし	脆弱性なし
12.2SCH	脆弱性なし	脆弱性なし
12.2SE	脆弱性なし	12.2(55)SE7 12.2(54)SE4までのリリースには脆弱性はありません。
12.2SEA	脆弱性なし	脆弱性あり。最初の修正はリリース15.0SE
12.2SEB	脆弱性なし	脆弱性あり。最初の修正はリリース15.0SE
12.2SEC	脆弱性なし	脆弱性あり。最初の修正はリリース15.0SE
12.2SED	脆弱性なし	脆弱性あり。最初の修正はリリース15.0SE
12.2SEE	脆弱性なし	脆弱性あり。最初の修正はリリース15.0SE
12.2SEF	脆弱性なし	脆弱性あり。最初の修正はリリース15.0SE
12.2SEG	脆弱性なし	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。最初の修正はリリース15.0SE
12.2SG	脆弱性なし	12.2(53)SG9
12.2SGA	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SG
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	脆弱性なし
12.2SQ	脆弱性なし	12.2(50)SQ5
12.2SRA	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRE
12.2SRB	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRE
12.2SRC	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRE

12.2SRD	脆弱性なし	脆弱性あり。最初の修正はリリース 12.2SRE
12.2SRE	12.2(33)SRE8	12.2(33)SRE8
12.2STE	脆弱性なし	脆弱性なし
12.2SU	脆弱性なし	脆弱性なし
12.2SV	脆弱性なし	Vulnerable.脆弱性が存在するのは、リリース12.2(25)SV2、12.2(27)SV5、および12.2(29)SV3だけです。
12.2SVA	脆弱性なし	脆弱性なし
12.2SVC	脆弱性なし	脆弱性なし
12.2SVD	脆弱性なし	脆弱性なし
12.2SVE	脆弱性なし	脆弱性なし
12.2SW	脆弱性なし	脆弱性あり。最初の修正はリリース 15.0M* 12.2(23)SW1までのリリースには脆弱性はありません。
12.2SX	脆弱性なし	脆弱性なし
12.2SXA	脆弱性なし	脆弱性なし
12.2SXB	脆弱性なし	脆弱性なし
12.2SXD	脆弱性なし	脆弱性なし
12.2SXE	脆弱性なし	脆弱性なし
12.2SXF	脆弱性なし	脆弱性なし
12.2SXH	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。
12.2SXI	脆弱性なし	12.2(33)SXI11
12.2日本語	脆弱性なし	12.2(33)SXJ5
12.2SY	脆弱性なし	12.2(50)SY4
12.2SZ	脆弱性なし	脆弱性なし
12.2T	脆弱性なし	脆弱性なし
12.2TPC	脆弱性なし	脆弱性なし
12.2WO	脆弱性なし	脆弱性なし
12.2XA	脆弱性なし	脆弱性なし
12.2XB	脆弱性なし	脆弱性なし
12.2XC	脆弱性なし	脆弱性なし
12.2XD	脆弱性なし	脆弱性なし

12.2XE	脆弱性なし	脆弱性なし
12.2XF	脆弱性なし	脆弱性なし
12.2XG	脆弱性なし	脆弱性なし
12.2XH	脆弱性なし	脆弱性なし
12.2XI	脆弱性なし	脆弱性なし
12.2XJ	脆弱性なし	脆弱性なし
12.2XK	脆弱性なし	脆弱性なし
12.2XL	脆弱性なし	脆弱性なし
12.2XM	脆弱性なし	脆弱性なし
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	脆弱性なし	12.2(54)XOより前のリリースには脆弱性があり、12.2(54)XO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12.2SG
12.2XQ	脆弱性なし	脆弱性なし
12.2XR	脆弱性なし	脆弱性なし
12.2XS	脆弱性なし	脆弱性なし
12.2XT	脆弱性なし	脆弱性なし
12.2XU	脆弱性なし	脆弱性なし
12.2XV	脆弱性なし	脆弱性なし
12.2XW	脆弱性なし	脆弱性なし
12.2YA	脆弱性なし	脆弱性なし
12.2YC	脆弱性なし	脆弱性なし
12.2YD	脆弱性なし	脆弱性なし
12.2YE	脆弱性なし	脆弱性なし
12.2YK	脆弱性なし	脆弱性なし

12.2YO	脆弱性なし	脆弱性なし
12.2YP	脆弱性なし	脆弱性なし
12.2YT	脆弱性なし	脆弱性なし
12.2YW	脆弱性なし	脆弱性なし
12.2YX	脆弱性なし	脆弱性なし
12.2YY	脆弱性なし	脆弱性なし
12.2YZ	脆弱性なし	脆弱性なし
12.2ZA	脆弱性なし	脆弱性なし
12.2ZB	脆弱性なし	脆弱性なし
12.2ZC	脆弱性なし	脆弱性なし
12.2ZD	脆弱性なし	脆弱性なし
12.2ZE	脆弱性なし	脆弱性なし
12.2ZH	脆弱性なし	脆弱性なし
12.2ZJ	脆弱性なし	脆弱性なし
12.2ZP	脆弱性なし	脆弱性なし
12.2ZU	脆弱性なし	脆弱性なし
12.2ZX	脆弱性なし	脆弱性なし
12.2ZY	脆弱性なし	脆弱性なし
12.2ZYA	脆弱性なし	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）	2013年3月の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 12.3 ベースのリリースはありません。		
Affected 12.4-Based Releases	First Fixed Release（修正された最初のリリース）	2013年3月の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 12.4 ベースのリリースはありません。		
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）	2013年3月の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
15.0EB	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。
15.0ED	脆弱性なし	脆弱性なし
15.0EY	脆弱性なし	脆弱性なし
15.0M	脆弱性なし	15.0(1)M10 *

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。
15.0秒	脆弱性あり。最初の修正はリリース15.1S 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。	脆弱性あり。最初の修正はリリース15.1S 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。
15.0SE	脆弱性なし	15.0(2)SE1
15.0SG	脆弱性なし 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。	脆弱性なし 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。
15.0SQA	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。	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	脆弱性なし	15.0(1)SY4
15.0XA	脆弱性なし	脆弱性あり。最初の修正はリリース15.1M
15.0XO	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。	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。
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）	2013年3月の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	脆弱性あり。最初の修正はリリース15.2S	脆弱性あり。最初の修正はリリース15.2S
15.1GC	脆弱性なし	15.1(4)GC1
1,510万	脆弱性なし	15.1(4)M6
15.1MR	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。
15.1MRA	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。

15.1S	15.1(3)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。	† 脚注を参照 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 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。	脆弱性なし 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。
15.1SNG	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。
15.1SNI	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。
15.1SVA	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。
15.1サービス	脆弱性なし	脆弱性なし
15.1SY	15.1(1)SY1（2013年5月24日に入手可能）	15.1(1)SY1（2013年5月24日に入手可能）
15.1T	脆弱性なし	脆弱性あり。最初の修正はリリース15.1M
15.1XB	脆弱性なし	脆弱性あり。最初の修正はリリース15.1M
Affected 15.2-Based Releases	First Fixed Release（修正された最初のリリース）	2013年3月の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	脆弱性なし	脆弱性あり。15.4Tの任意のリリースに移行
15.2GCA	脆弱性なし	脆弱性あり。15.4Tの任意のリリースに移行
15.2JA	脆弱性なし	15.2(2)JA
15.2JAX	脆弱性なし	脆弱性なし

15.2JB	脆弱性なし	脆弱性なし
15.2JN	脆弱性なし	脆弱性なし
1,520万	脆弱性なし	15.2(4)M3
15.2秒	15.2(4)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。	15.2(4)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。
15.2SA	15.2(2)SA	15.2(2)SA
15.2SNG	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。
15.2SNH	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。
15.2SNI	脆弱性なし	脆弱性なし
15.2T	脆弱性なし	15.2(1)T4（2013年5月3日に入手可能） 15.2(2)T3 15.2(3)T3
Affected 15.3-Based Releases	First Fixed Release（修正された最初のリリース）	2013年3月の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
影響を受ける 15.3 ベースのリリースはありません。		

* Cisco IOSソフトウェアリリース15.0Mは、2013年4月1日にソフトウェアメンテナンスが終了し、追加のリビルドは行われません。詳細については、 サポート終了通知を参照してください。Cisco IOSソフトウェアリリース15.1Mへの移行を検討することをお勧めします。

† Cisco 7600シリーズルータの場合、2013年3月のバンドル公開に含まれるすべてのシスコセキュリティアドバイザリに対する最初の修正リリースは、Cisco IOSソフトウェアリリース15.1(3)S5です。Cisco 7200および7300シリーズルータの場合、2013年3月の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済みリリースは、Cisco IOSソフトウェアリリース15.1(3)S5aであり、2013年4月15日から利用可能になります。

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	First Fixed Release（修正さ	2013年3月のCisco IOSソフトウェアセキュ

ウェア リリース	れた最初のリリース）	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	脆弱性なし	脆弱性なし
2.2.x	脆弱性なし	脆弱性なし
2.3.x	脆弱性なし	脆弱性なし
2.4.x	脆弱性なし	脆弱性なし
2.5.x	脆弱性なし	脆弱性なし
2.6.x	脆弱性なし	脆弱性なし
3.1.xS	3.4.5S	脆弱性あり。3.4.5S以降に移行してください。
3.1.xSG	脆弱性なし	脆弱性なし
3.2.xS	3.4.5S	脆弱性あり。3.4.5S以降に移行してください。
3.2.xSE	脆弱性なし	脆弱性なし
3.2.xSG	脆弱性なし	脆弱性なし
3.2.XO	脆弱性なし	脆弱性なし
3.2.xSQ	脆弱性なし	脆弱性なし
3.3.xS	3.4.5S	脆弱性あり。3.4.5S以降に移行してください。
3.3xSG	脆弱性なし	脆弱性なし
3.4.xS	3.4.5S	脆弱性あり。3.4.5S以降に移行してください。
3.4.xSG	脆弱性なし	脆弱性なし
3.5.xS	3.7.2S	脆弱性あり。3.7.2S以降に移行してください。
3.6.xS	3.7.2S	脆弱性あり。3.7.2S以降に移行してください。
3.7.xS	3.7.2S	3.7.2S
3.8.xS	脆弱性なし	脆弱性なし
3.9.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、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、シスコの社内テストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-rsvp

改訂履歴

リビジョン 1.2	2013年 4月11日	15.0SEおよび15.0SGトレインの脆弱性ステータスを更新。
リビジョン 1.1	2013年 3月28日	「ソフトウェアバージョンと修正」セクションの修正済みソフトウェアの表を更新。
リビジョン 1.0	2013年 3月27日	初回公開リリース

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。

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。