Cisco IOSソフトウェアプロトコル変換の脆弱性

アドバイザリーID : cisco-sa-20130327-pt　CVE-2013-1147
初公開日 : 2013-03-27 16:00
最終更新日 : 2013-04-11 15:23
バージョン 1.1 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID : CSCtz35999

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ソフトウェアプロトコル変換(PT)機能には、認証されていないリモートの攻撃者がサービス妨害(DoS)状態を引き起こす可能性のある脆弱性が含まれています。

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。 この脆弱性に対しては回避策があります。

このアドバイザリは次のリンクで確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-pt

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

この脆弱性は、該当バージョンのCisco IOSソフトウェアを実行していて、脆弱性のあるプロトコ

ル変換コンフィギュレーションまたはTelnet-to-PADプロトコル変換ルールセットが設定されているデバイスに影響を与えます。

脆弱性のある製品

ワンステップのプロトコル変換が構成され、既定の着信接続ポート番号（Telnetポート23）が使用されている場合、脆弱性のあるプロトコル変換構成が発生します。ワンステップのプロトコル変換の着信接続ポート番号が既定以外のポートに対して構成されている場合、そのデバイスは脆弱性の影響を受けません。

脆弱性のあるプロトコル変換設定を特定するには、デバイスにログインして、 show translateコマンドラインインターフェイス(CLI)コマンドを発行します。 次の例は、デフォルトの着信接続ポート番号が設定された少なくとも1つの着信TCP/IPプロトコル変換接続によるプロトコル変換用に設定されたデバイスを示しています。出力に、ポート23がリストされている変換エントリが含まれていない場合、そのデバイスには脆弱性はありません。次の出力は、脆弱性のある設定のデバイスを示しています。

```
<#root>

Terminal_Server#show translate

Translate From:

TCP

 192.168.0.1

Port 23


          To:   X25 1234
          0/0 users active, 0 peak, 0 total, 0 failures

Translate From: TCP 192.168.100.25 Port 1025
          To:   X25 1235
          0/0 users active, 0 peak, 0 total, 0 failures
Terminal_Server#
```

次に、脆弱性のない設定のデバイスを示します。

```
Terminal_Server#show translate

Translate From: TCP 192.168.0.1 Port 1025
          To:   X25 1234
          0/0 users active, 0 peak, 0 total, 0 failures

Translate From: TCP 192.168.100.25 Port 1026
          To:   X25 1235
          0/0 users active, 0 peak, 0 total, 0 failures
Terminal_Server#
```

Telnet-to-PADプロトコル変換ルールセット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 CLIコマンドを発行します。出力に設定コマンド translate use telnet <ip address>が含まれており、また telnet to padコマンドでルールセットが定義されている場合、そのデバイスには脆弱性が存在します。次の例は、脆弱性のあるTelnet-to-PADプロトコル変換ルールセットの設定を示しています。

<#root>

```
Terminal_Server#show running-config | begin use telnet
translate
```

use telnet

```
 192.168.0.1
translate ruleset example_ruleset from
```

telnet to pad

```
 description *** example translation ruleset ***
 match source-addr 192.168.100.1
 set pad dest-addr 4321
<rest of output removed for brevity>
Terminal_Server#
```

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

次の製品には脆弱性が存在しないことが確認されています。

- Cisco IOS XE ソフトウェア
- Cisco IOS XR ソフトウェア
- Cisco NX-OS ソフトウェア

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ソフトウェアには、認証されていないリモートの攻撃者がサービス妨害(DoS)状態を引き起こす可能性のある脆弱性が存在します。

この脆弱性は、該当ソフトウェアで脆弱性のあるプロトコル変換設定が使用されている場合に、TCP接続情報の検証が不十分であることに起因します。攻撃者は、該当デバイスの該当プロトコル変換リソースへの接続を試みることにより、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者は該当デバイスのリロードを引き起こす可能性があります。

この脆弱性を不正利用するためにTCP 3ウェイハンドシェイクは必要ありません。 通過トラフィックによって、この脆弱性が引き起こされることはありません。

この脆弱性は、Cisco Bug ID CSCtz35999(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-2013-1147が割り当てられています。

回避策

この脆弱性を軽減するには、次の回避策があります。

着信接続のデフォルトポート番号の変更

デフォルトの着信接続ポート番号を使用して1ステップのプロトコル変換が設定されているデバイスの場合、管理者はデフォルトの着信接続ポート番号をポート23以外の適切な値に変更できます。次の例は、デフォルトの着信接続ポート番号の変更を示しています。
脆弱性のある元の設定：

```
translate tcp 192.168.0.3 x25 1234
```

デフォルトの着信接続ポート番号の設定が変更されました。

```
translate tcp 192.168.0.3 port 1025 x25 1234
```

ルールセット内のポートのスキップ

ルールセットを使用する場合は、ポート514および544を無視します。

```
translate ruleset example_ruleset from telnet to pad
description *** example translation using a ruleset ***
match source-addr 192.168.0.1
set pad dest-addr 1234
skip dest-port 514
skip dest-port 544
```

インフラストラクチャ アクセス コントロール リスト

ネットワークを通過するトラフィックをブロックするのは往々にして困難ですが、インフラストラクチャデバイスに送られてはならないトラフィックを特定し、ネットワークの境界でそのトラフィックをブロックすることは可能です。インフラストラクチャアクセスコントロールリスト(iACL)は、ネットワークセキュリティのベストプラクティスと考えられており、ここでの特定の脆弱性の回避策としてだけでなく、優れたネットワークセキュリティへの長期的な付加機能として考慮する必要があります。次のACLの例は、設定されたプロトコル変換の着信IPアドレスの範囲内のIPアドレスを持つすべてのデバイスを保護するために配備されたインフラストラクチャアクセスリストの一部として含める必要があります。

Cisco IOSを実行するデバイスのアクセスリストの例を次に示します。

```
! – 送信元が514|544のプロトコル変換サービスパケットを拒否します。
access-list 150 deny tcp any CONFIGURED_PROTOCOL_TRANSLATION_ADDRESSES MASK eq 514
access-list 150 deny tcp any CONFIGURED_PROTOCOL_TRANSLATION_ADDRESSES MASK eq 544

! – 他のすべてのトラフィックがこのデバイスを通過することを許可します。
access-list 150 permit ip any any
interface serial2/0
  ip access-group 150 in
```

ホワイトペーパー『Protecting Your Core: Infrastructure Protection Access Control Lists』には、アクセスリストによるインフラストラクチャ保護のガイドラインと推奨される導入方法が記載されています。このWhite Paperは http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtmlにあります。

ネットワーク内のシスコデバイスに適用可能な他の対応策は、https://sec.cloudapps.cisco.com/security/center/viewAMBAlert.x?alertId=28001で入手できる付属ドキュメント『Identifying and Mitigating Exploitation of the Cisco IOS Software Protocol Translation Vulnerability』で参照できます。

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
影響を受ける 12.2 ベースのリリースはありません。		

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
12.3	脆弱性なし	脆弱性なし
12.3B	脆弱性なし	脆弱性なし
12.3BC	脆弱性なし	脆弱性なし
12.3BW	脆弱性なし	脆弱性なし
12.3JA	脆弱性なし	脆弱性なし
12.3JEA	脆弱性なし	脆弱性なし
12.3JEB	脆弱性なし	脆弱性なし
12.3JEC	脆弱性なし	脆弱性なし
12.3JED	脆弱性なし	脆弱性なし
12.3JEE	脆弱性なし	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。 12.3(8)JK1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*	12.3(2)JK3 までのリリースには脆弱性はありません。12.3(8)JK1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*
12.3JL	脆弱性なし	脆弱性なし
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15.0M* 12.3(7)T12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15.0M* 12.3(2)T9までのリリースには脆弱性はありません。
12.3TPC	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。
12.3XA	脆弱性なし	脆弱性なし
12.3XB	脆弱性なし	脆弱性なし
12.3XC	脆弱性なし	脆弱性なし
12.3XD	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M*
12.3XE	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M*
12.3XF	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。
12.3XG	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M*

12.3XI	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SB
12.3XJ	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M*
12.3XK	脆弱性なし	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15.0M*	脆弱性あり。最初の修正はリリース15.0M*
12.3XQ	脆弱性なし	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15.0M* 12.3(7)XR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15.0M*
12.3XU	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M*
12.3XW	脆弱性あり。12.4XNの任意のリリースに移行	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15.0M* 12.3(8)XX1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15.0M*
12.3XY	脆弱性なし	脆弱性なし
12.3XZ	脆弱性なし	脆弱性なし
12.3YD	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M*
12.3YF	注：12.3(11)YF1より前のリリースには脆弱性があり、12.3(11)YF1以降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15.0M*
12.3YG	脆弱性あり。最初の修正はリリース15.0M*	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15.0M*	脆弱性あり。最初の修正はリリース15.0M*
12.3YJ	脆弱性なし	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15.0M*	脆弱性あり。最初の修正はリリース15.0M*
12.3YM	12.3(14)YM10までのリリースには脆弱性はありません。 12.3(14)YM12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*	脆弱性あり。最初の修正はリリース15.0M*
12.3YQ	脆弱性なし	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15.0M*	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	脆弱性あり。最初の修正はリリース15.0M*

	15.0M*	
12.3YU	脆弱性あり。最初の修正はリリース15.0M* 12.3(14)YU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15.0M*
12.3YX	リリース12.3(14)YX4および12.3(14)YX9には脆弱性があり、リリース12.3(14)YX10以降には脆弱性はありません。12.4XNの任意のリリースに移行します。	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。最初の修正はリリース15.0M*	脆弱性あり。最初の修正はリリース15.0M*
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
12.4	脆弱性あり。最初の修正はリリース15.0M*	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	脆弱性なし	脆弱性なし
12.4JAL	脆弱性なし	脆弱性なし
12.4ジャム	脆弱性なし	12.4(25e)JAMより前のリリースには脆弱性があり、12.4(25e)JAM以降のリリースには脆弱性はありません。 12.4JAN12.4(25e)JAMの任意のリリースに移行
12.4JAX	脆弱性なし	脆弱性なし
12.4JAZ	脆弱性なし	脆弱性なし
12.4JDA	脆弱性なし	脆弱性なし
12.4JDC	脆弱性なし	脆弱性なし
12.4JDD	脆弱性なし	脆弱性なし
12.4JDE	脆弱性なし	脆弱性なし
12.4JHA	脆弱性なし	脆弱性なし

12.4JHB	脆弱性なし	脆弱性なし
12.4JHC	脆弱性なし	脆弱性なし
12.4JK	脆弱性なし	脆弱性なし
12.4JL	脆弱性なし	脆弱性なし
12.4JX	脆弱性なし	脆弱性なし
12.4JY	脆弱性なし	脆弱性なし
12.4JZ	脆弱性なし	脆弱性なし
12.4MD	脆弱性なし	脆弱性あり。最初の修正はリリース 12.4MDB
12.4MDA	脆弱性なし	脆弱性あり。最初の修正はリリース 12.4MDB
12.4MDB	脆弱性なし	12.4(24)MDB13
12.4MR	12.4(12)MR1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。
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 15.0M*	脆弱性あり。最初の修正はリリース15.0M*
12.4SW	12.4(15)SW9aより前のリリースには脆弱性があり、12.4(15)SW9a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*	脆弱性あり。最初の修正はリリース15.0M*
12.4T	脆弱性あり。最初の修正はリリース 15.0M*	脆弱性あり。最初の修正はリリース15.0M*
12.4XA	脆弱性あり。最初の修正はリリース 15.0M*	脆弱性あり。最初の修正はリリース15.0M*
12.4XB	12.4(2)XB5までのリリースには脆弱性はありません。 リリース12.4(2)XB7以降には脆弱性はありません。最初の修正はリリース 15.0M*	脆弱性あり。最初の修正はリリース15.0M*
12.4XC	脆弱性あり。最初の修正はリリース 15.0M*	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 15.0M*	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15.0M*	脆弱性あり。最初の修正はリリース15.0M*
12.4XF	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M*
12.4XG	12.4(9)XG1までのリリースには脆弱性はありません。 12.4(9)XG3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*	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15.0M*	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15.0M*	脆弱性あり。最初の修正はリリース15.0M*
12.4XL	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。
12.4XM	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M*
12.4XN	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。
12.4XP	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。
12.4XQ	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M*
12.4XR	脆弱性なし	脆弱性あり。最初の修正はリリース15.0M*
12.4XT	脆弱性あり。最初の修正はリリース15.0M*	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15.0M*	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15.0M*	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15.0M*	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15.0M*	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。
12.4YE	脆弱性なし	12.4(24)YE3e
12.4YG	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。
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	15.0(1)M10 *	15.0(1)M10 *
15.0MR	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。
15.0秒	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	脆弱性あり。最初の修正はリリース15.1M	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	脆弱性なし	脆弱性あり。最初の修正はリリース15.2S
15.1GC	15.1(4)GC1	15.1(4)GC1
1,510万	15.1(4)M6	15.1(4)M6
15.1MR	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。
15.1MRA	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。
15.1S	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。	15.1(3)S5 † 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。	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。
15.1SNH	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。
15.1SNI	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。
15.1SVA	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。
15.1サービス	脆弱性なし	脆弱性なし
15.1SY	脆弱性なし	15.1(1)SY1（2013年5月24日に入手可能）
15.1T	脆弱性あり。最初の修正はリリース15.1M	脆弱性あり。最初の修正はリリース15.1M
15.1XB	脆弱性あり。最初の修正はリリース15.1M	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	脆弱性あり。15.4Tの任意のリリースに移行	脆弱性あり。15.4Tの任意のリリースに移行
15.2GCA	脆弱性あり。15.4Tの任意のリリースに移行	脆弱性あり。15.4Tの任意のリリースに移行
15.2JA	15.2(2)JA1 15.2(4)JA（2013年4月29日に入手可能）	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	15.2(4)M3	15.2(4)M3
15.2秒	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。	15.2(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	脆弱性なし	15.2(2)SA
15.2SNG	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。
15.2SNH	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。
15.2SNI	脆弱性なし	脆弱性なし
15.2T	15.2(1)T4（2013年5月3日に入手可能） 15.2(2)T3 15.2(3)T3	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
15.3秒	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。
15.3T	15.3(1)T1（2013年3月29日に入手可能） 15.3(2)T（2013年3月29日に入手可能）	15.3(1)T1(29-MAR-1315.3(2)Tに利用可能)、29-MAR-13に利用可能

* 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せん。

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、お客様のサービスリクエストの対応時に発見されました。

URL

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

改訂履歴

リビジョン 1.1	2013年4月11日	「bundle first fixed」列の15.0EYのデータを更新。
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

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。