Cisco IOSソフトウェアIPバージョン6 overマルチプロトコルラベルスイッチングの脆弱性

アドバイザリーID : cisco-sa-20110928-ipv6mpls
初公開日 : 2011-09-28 16:00
最終更新日 : 2012-09-21 19:20
バージョン 1.2 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID : CSCtj30155 CSCto07919

CVE-2011-3282
CVE-2011-3274

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ソフトウェアは、Multiprotocol Label Switching（MPLS；マルチプロトコルラベルスイッチング）ドメインでIPバージョン6(IPv6)パケットを処理する際にCisco IOSデバイスのリロードを引き起こす2つの脆弱性の影響を受けます。これらの脆弱性は次のとおりです。

- 巧妙に細工されたIPv6パケットによりMPLS設定デバイスがリロードされる可能性
- ICMPv6パケットによりMPLS設定デバイスがリロードする場合がある

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。

これら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、https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6mpls で公開されています。

注： 2011年9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10件のCisco Security Advisoryが含まれています。9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、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、2011年9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: 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_sep11.html

該当製品

脆弱性のある製品

脆弱性のあるバージョンのCisco IOSソフトウェアを実行し、MPLSが設定されているCisco IOSソフトウェアまたはCisco IOS XEソフトウェアデバイス（以降、このドキュメントではCisco IOSソフトウェアと表記します）は、MPLSドメインを通過するIPv6トラフィックに関連する2つの脆弱性の影響を受けます。2つの脆弱性は互いに独立しています。

注：該当するデバイス自体でIPv6を設定する必要はありません。この脆弱性を悪用するには、MPLSラベルスイッチドパケットに特定のIPv6ペイロードが含まれている必要があります。

デバイスでMPLS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、コマンドラインインターフェイス(CLI)コマンドshow mpls interfaceを発行します。IPの状態がYesの場合、そのデバイスには脆弱性が存在します。次の例は、インターフェイスEthernet0/0にMPLSが設定されているデバイスを示しています。

```
Router#show mpls interface
Interface       IP           Tunnel  BGP  Static  Operational
Ethernet0/0   Yes (ldp)    No      No   No       Yes
Router#
```

次の2つの例は、MPLSフォワーディングが無効になっているデバイスからの応答を示しています。最初の例は、インターフェイスが返されないことを示しています。

```
router#show mpls interface
Interface              IP            Tunnel   BGP Static Operational
routers#
```

2番目の例では、MPLS転送が設定されていないことを示すメッセージがデバイスに表示されます。

```
router#show mpls interface
no MPLS apps enabled or MPLS not enabled on any interfaces

router#
```

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 (fc1)
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、ホワイトペーパー『Cisco IOS and NX-OS Software Reference Guide』(http://www.cisco.com/web/about/security/intelligence/ios-ref.html)を参照してください。

脆弱性を含んでいないことが確認された製品

MPLSが設定されていないデバイスには脆弱性は存在しません。

次の製品は、これらの脆弱性の影響を受けないことが確認されています。

- Cisco IOS XR 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

MPLSネットワーク内のパケット処理ノードは、プロバイダールータ（Pルータ）およびプロバイダーエッジルータ（PEルータ）と呼ばれ、MPLSで設定されます。PルータとPEルータの両方が、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。

MPLSが有効で、IPv6ペイロードを含むMPLSラベルスイッチドパケットを伝送できるネットワークでは、特定のIPv6ペイロードを含むMPLSラベルスイッチドパケットを処理するときにデバイスがクラッシュする可能性があります。これらの脆弱性の影響を受ける一般的な導入シナリオは、Cisco IPv6 Provider Edge Router(6PE)またはIPv6 VPN Provider Edge Router(6VPE)です。

巧妙に細工されたIPv6パケットによりMPLS設定デバイスがリロードされる可能性

巧妙に細工されたIPv6パケットは、Cisco IOSソフトウェアによってパケットが処理されるときに、MPLS TTLが期限切れになったためにデバイスがクラッシュする可能性があります。この脆弱性を不正利用するために使用される巧妙に細工されたパケットは、MPLSラベルが付いていないインターフェイスで受信されると、通知なしにCisco IOSソフトウェアで廃棄されます。

この脆弱性は、Cisco Bug ID CSCto07919(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-2011-3274が割り当てられています。

ICMPv6パケットによりMPLS設定デバイスがリロードする場合がある

MPLS TTLが期限切れになったため、Cisco IOSソフトウェアによってパケットが処理されると、有効なICMPv6パケットによってデバイスがクラッシュする場合があります。この脆弱性を不正利用するために使用されるパケットは、パケットにMPLSラベルが付いていないインターフェイスで受信されても、Cisco IOSソフトウェアには影響しません。

この脆弱性は、Cisco Bug ID CSCtj30155(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2011-3282が割り当てられています。

回避策

両方の脆弱性に対して、次の回避策が適用されます。

MPLS TTLプロパゲーションの無効化

MPLS TTLプロパゲーションを無効にすると、これらの脆弱性のエクスプロイトを防止できます。MPLS TTLプロパゲーションは、MPLSドメインのすべてのPEルータで無効にする必要があります。MPLS TTLプロパゲーションを無効にするには、グローバルコンフィギュレーションコマンドno mpls ip propagate-ttlを入力します。no mpls ip propagate-ttl forwardだけが設定されている場合でも、MPLSドメイン内からこの脆弱性が悪用される可能性があります。

MPLS TTL propagationコマンドの詳細については、http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_m1.html#wp1013846にある設定ガイドを参照してください。

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せください。

また、Cisco IOS Software Checkerは、https://sec.cloudapps.cisco.com/security/center/selectIOSVersion.xのCisco Security(SIO)ポータルでも入手できます。特定のバージョンのCisco IOSソフトウェアに影響を与えるセキュリティアドバイザリを確認するための機能がいくつかあります。

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「このアドバイザリの最初の修正済みリリース」列に記載されます。2011年9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には、Cisco IOSソフトウェアセキュリティアドバイザリのバンドル公開に含まれるすべての公開済みの脆弱性を修正する最初の修正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。

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	このアドバイザリの最初の修正リリース	2011年9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 12.1-Based Releases	このアドバイザリの最初の修正リリース	2011年9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

12.1E	脆弱性なし	12.2(18)SXF17b
Affected 12.2-Based Releases	このアドバイザリの最初の修正リリース	2011年9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	脆弱性あり。最初の修正はリリース12.4
12.2B	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.2BC	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.2BW	脆弱性なし	脆弱性なし
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	脆弱性なし
12.2BZ	脆弱性なし	脆弱性なし
12.2CX	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.2CY	脆弱性なし	脆弱性なし
12.2CZ	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SB

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	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。
12.2EX	脆弱性なし	12.2(55)EX3
12.2EY	脆弱性なし	12.2(58)EY
12.2EZ	脆弱性なし	脆弱性あり。 15.0SEの任意のリリースに移行
12.2FX	脆弱性なし	脆弱性あり(最初の修正はリリース12.2SE)
12.2FY	脆弱性なし	脆弱性あり(最初の修正はリリース12.2EX)

12.2FZ	脆弱性なし	脆弱性あり(最初の修正はリリース12.2SE)
12.2IRA	脆弱性なし	脆弱性あり。 12.2IRGの任意のリリースに移行
12.2IRB	脆弱性なし	脆弱性あり。 12.2IRGの任意のリリースに移行
12.2IRC	脆弱性なし	脆弱性あり。 12.2IRGの任意のリリースに移行
12.2IRD	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。
12.2IRE	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。
12.2IRF	脆弱性なし	脆弱性あり。 12.2IRGの任意のリリースに移行
12.2IRG	脆弱性なし	脆弱性なし

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	脆弱性なし
12.2MC	脆弱性なし	脆弱性あり。最初の修正はリリース12.4

12.2MRA	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRD
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	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12.2SB
12.2SB	脆弱性なし	12.2(31)SB20 12.2(33)SB10
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12.2SCC
12.2SCB	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SCC
12.2SCC	脆弱性なし	12.2(33)SCC7

12.2SCD	脆弱性なし	12.2(33)SCD6
12.2SCE	脆弱性なし	12.2(33)SCE1 12.2(33)SCE2
12.2SCF	脆弱性なし	脆弱性なし
12.2SE	脆弱性なし	12.2(55)SE3 12.2(58)SE
12.2SEA	脆弱性なし	脆弱性あり(最初の修正はリリース12.2SE)
12.2SEB	脆弱性なし	脆弱性あり(最初の修正はリリース12.2SE)
12.2SEC	脆弱性なし	脆弱性あり(最初の修正はリリース12.2SE)
12.2SED	脆弱性なし	脆弱性あり(最初の修正はリリース12.2SE)
12.2SEE	脆弱性なし	脆弱性あり(最初の修正はリリース12.2SE)
12.2SEF	脆弱性なし	脆弱性あり(最初の修正はリリース12.2SE)
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12.2EX
12.2SG	脆弱性なし	12.2(53)SG4より前のリリースには脆弱性があり、12.2(53)SG4以降のリリースには脆弱性はありません。
12.2SGA	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。
12.2SL	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	脆弱性なし
12.2SQ	脆弱性なし	12.2(50)SQ3
12.2SRA	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRD

12.2SRB	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRD
12.2SRC	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRD
12.2SRD	脆弱性なし	12.2(33)SRD6
12.2SRE	12.2(33)SRE4	12.2(33)SRE4
12.2STE	脆弱性なし	脆弱性なし
12.2SU	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.2SV	脆弱性なし	12.2(29a)SVより前のリリースには脆弱性があり、12.2(29a)SV以降のリリースには脆弱性はありません。12.2SVDの任意のリリースに移行
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。
12.2SX	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SXF
12.2SXA	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SXF
12.2SXB	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SXF
12.2SXD	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SXF
12.2SXE	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SXF
12.2SXF	脆弱性なし	12.2(18)SXF17b
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)SXI6

12.2日本語	脆弱性なし	12.2(33)SXJ1
12.2SY	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。
12.2SZ	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SB
12.2T	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
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	脆弱性なし
12.2XB	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
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
12.2XN	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」	「Cisco IOS-XEソフトウェアの可用性」を

	を参照してください。	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。
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	脆弱性あり。最初の修正はリリース12.4
12.2YB	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
12.2YF	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。
12.2YG	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。
12.2YH	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。
12.2YJ	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	脆弱性なし
12.2YL	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。
12.2YM	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.2YN	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	脆弱性なし

12.2YP	脆弱性なし	脆弱性なし
12.2YQ	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。
12.2YR	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。
12.2YS	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。
12.2YT	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。
12.2YU	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。
12.2YV	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	脆弱性あり。最初の修正はリリース12.2SXF
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	脆弱性なし
12.2ZD	脆弱性なし	脆弱性なし
12.2ZE	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.2ZF	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.2ZG	脆弱性なし	脆弱性なし
12.2ZH	脆弱性なし	脆弱性あり。最初の修正はリリース12.4

12.2ZJ	脆弱性なし	脆弱性なし
12.2ZL	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	脆弱性なし
12.2ZU	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SXH
12.2ZX	脆弱性なし	脆弱性なし
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	このアドバイザリの最初の修正リリース	2011年9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

Releases		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	このアドバイザリの最初の修正リリース	2011年9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	このアドバイザリの最初の修正リリース	2011年9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
15.0M	15.0(1)M7	15.0(1)M7
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)S4 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)S4 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。
15.0SE	脆弱性なし	脆弱性なし
15.0SG	「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。
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	「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。
影響を受ける 15.1 ベースのリリース	このアドバイザリの最初の修正リリース	2011年9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。
15.1GC	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)
1,510万	15.1(4)M1	15.1(4)M2（2011年9月30日に入手可能）
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。
15.1S	15.1(2)S2 15.1(3)S 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(2)S2 15.1(3)S 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。
15.1T	15.1(1)T4（2011年12月9日に入手可能） 15.1(2)T4 15.1(3)T2	15.1(1)T4（2011年12月9日に入手可能） 15.1(2)T4 15.1(3)T2

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	このアドバイザリの最初の修正リリース	2011年9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15.2ベースのリリースはありません		

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リリース	このアドバイザリの最初の修正リリース	2011年9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
2.1.x	脆弱性あり、3.3.2S以降に移行	脆弱性あり、3.3.2S以降に移行
2.2.x	脆弱性あり、3.3.2S以降に移行	脆弱性あり、3.3.2S以降に移行
2.3.x	脆弱性あり、3.3.2S以降に移行	脆弱性あり、3.3.2S以降に移行
2.4.x	脆弱性あり、3.3.2S以降に移行	脆弱性あり、3.3.2S以降に移行

2.5.x	脆弱性あり、3.3.2S以降に移行	脆弱性あり、3.3.2S以降に移行
2.6.x	脆弱性あり、3.3.2S以降に移行	脆弱性あり、3.3.2S以降に移行
3.1.xS	3.1.4S	脆弱性あり、3.3.2S以降に移行
3.1.xSG	脆弱性なし	脆弱性あり、3.2.0SG以降に移行
3.2.xS	脆弱性あり、3.3.2S以降に移行	脆弱性あり、3.3.2S以降に移行
3.2.xSG	脆弱性なし	脆弱性なし
3.3.xS	3.3.2S	3.3.2S
3.4.xS	脆弱性なし	脆弱性なし

Cisco IOSリリースへのCisco IOS XE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。

Cisco IOS XRソフトウェアは、2011年9月の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

このアドバイザリで説明されている脆弱性の公表や悪用に関する情報は Cisco PSIRT には寄せられていません。

これらの脆弱性は、カスタマーサポートコールの対応時に発見されたものです。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6mpls

改訂履歴

リビジョン 1.2	2011年 9月30日	Cisco IOSソフトウェアテーブルバンドル公開の最初の修正情報を更新。
リビジョン 1.1	2011年 9月28日	リリース15.0Sおよび15.1Sの修正済みCisco IOSソフトウェアテーブルに不足している情報を追加。
リビジョン 1.0	2011年 9月28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。