

# Cisco IOSソフトウェアのIPv6におけるDoS脆弱性



アドバイザリーID : cisco-sa-20110928-ipv6 [CVE-2011-](#)

初公開日 : 2011-09-28 16:00 [0944](#)

最終更新日 : 2014-05-20 12:47

バージョン 1.1 : Final

CVSSスコア : [7.8](#)

回避策 : No Workarounds available

Cisco バグ ID : [CSCtj41194](#)

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、IPバージョン6(IPv6)プロトコルスタックの実装に関する脆弱性が存在します。これにより、認証されていないリモートの攻撃者が、IPv6操作が有効になっている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。この脆弱性は、該当デバイスが不正なIPv6パケットを処理すると発生します。

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。

このアドバイザリーは、

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6> 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ーバンドル公開には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。各アドバイザリーには、このアドバイザリー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](http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep11.html)

## 該当製品

この脆弱性は、Cisco IOSソフトウェアを実行し、IPv6動作用に設定されているデバイスに影響を与えます。Cisco IOSソフトウェアでは、IPv6はデフォルトで有効になっていません。

### 脆弱性のある製品

該当するバージョンのCisco IOSソフトウェアを実行し、IPv6動作用に設定されているシスコデバイスが影響を受けます。Cisco IOSソフトウェアが稼働していて、IPv6が有効になっているデバイスでは、show ipv6 interface briefコマンドを実行すると、IPv6アドレスが割り当てられたインターフェイスがいくつか表示されます。

show ipv6 interface briefコマンドは、実行バージョンのCisco IOSソフトウェアがIPv6をサポートしていない場合はエラーメッセージを生成し、IPv6が無効の場合はIPv6アドレスを持つインターフェイスを表示しません。システムは、これらのシナリオのいずれにおいても脆弱ではありません。

IPv6が設定されたシステムでのshow ipv6 interface briefコマンドの出力例を次に示します。

```
router>show ipv6 interface brief
FastEthernet0/0          [up/up]
    FE80::222:90FF:FEB0:1098
    2001:DB8:2:93::3
    200A:1::1
FastEthernet0/1          [up/up]
    FE80::222:90FF:FEB0:1099
    2001:DB8:2:94::1
Serial0/0/0              [down/down]
    unassigned
Serial0/0/0.4            [down/down]
    unassigned
Serial0/0/0.5            [down/down]
    unassigned
Serial0/0/0.6            [down/down]
    unassigned
```

または、インターフェイスコンフィギュレーションコマンドipv6 address <IPv6 address>またはipv6 enableが設定に存在する場合は、IPv6プロトコルが有効になります。両方が存在する可能性があります。次の例の脆弱性のある設定は、この両方を示しています。

```
interface FastEthernet0/1
  ipv6 address 2001:0DB8:C18:1::/64 eui-64
  !
interface FastEthernet0/2
  ipv6 enable
```

Cisco IOSソフトウェアが稼働していて、物理インターフェイスまたは論理インターフェイスでIPv6が有効になっているデバイスは、ipv6 unicast-routingがグローバルに無効になっている（つまり、デバイスがIPv6パケットをルーティングしていない）場合でも脆弱です。管理者は show ipv6 interface brief コマンドを使用して、任意のインターフェイスでIPv6が有効になっているかどうかを確認できます。

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。

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、次のURLにある『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>。

### 脆弱性を含んでいないことが確認された製品

Cisco IOS XRソフトウェアおよびCisco IOS XEソフトウェアは、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

IPv6はInternet Engineering Task Force ( IETF ; インターネット技術特別調査委員会 ) によって設計されたもので、現在のバージョンであるIPバージョン4(IPv4)に代わるものです。

脆弱性は、Cisco IOSソフトウェアがIPv6パケットを処理する際に存在します。攻撃者は、IPv6トラフィックを処理するように設定された物理インターフェイスまたは論理インターフェイスに不正なIPv6パケットを送信することで、この脆弱性を不正利用する可能性があります。通過トラフィックでは、この脆弱性は引き起こされません。この脆弱性が悪用されると、該当するシステムが再起動する可能性があります。

この脆弱性は、Cisco Bug ID [CSCtj41194](#)(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-2011-0944が割り当てられています。

## 回避策

IPv6の設定が必要な場合は、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

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	First Fixed Release (修正された最初のリリース)	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	First Fixed Release ( 修正 された最初の 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	脆弱性あり。最初の修正は <a href="#">リ リース12.2SXF</a>
Affected 12.2- Based Releases	First Fixed Release ( 修正 された最初の 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 <a href="#">リ リース12.4</a>
12.2B	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リ リース12.4</a>
12.2BC	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リ リース12.4</a>
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 <a href="#">リ リース12.2SB</a>
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 <a href="#">リリース12.4</a>
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 <a href="#">リリース12.2SB</a>
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。このアドバイザーの <a href="#">「修正済みソフトウェアの取得」</a> 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 <a href="#">リリース12.2SE</a>
12.2FY	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.2EX</a>
12.2FZ	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.2SE</a>
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「 <a href="#">修正済みソフトウェアの取得</a> 」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「 <a href="#">修正済みソフトウェアの取得</a> 」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「 <a href="#">修正済みソフトウェアの取得</a> 」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「 <a href="#">修正済みソフトウェアの取得</a> 」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	脆弱性あり。このアドバイザリの「 <a href="#">修正済みソフトウェアの取得</a> 」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「 <a href="#">修正済みソフトウェアの取得</a> 」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「 <a href="#">修正済みソフトウェアの取得</a> 」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「 <a href="#">修正済みソフトウェアの取得</a> 」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。このアドバイザーの「 <a href="#">修正済みソフトウェアの取得</a> 」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。このアドバイザーの「 <a href="#">修正済みソフトウェアの取得</a> 」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 <a href="#">リリース12.4</a>
12.2MRA	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.2SRD</a>
12.2MRB	脆弱性なし	脆弱性が存在します。このアドバイザーの「 <a href="#">修正済みソフトウェアの取得</a> 」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 <a href="#">リリース12.2SB</a>

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 <a href="#">リリース12.2SB</a>
12.2SCA	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.2SCC</a>
12.2SCB	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.2SCC</a>
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 <a href="#">リリース12.2SE</a>
12.2SEB	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.2SE</a>
12.2SEC	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.2SE</a>

12.2SED	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.2SE</a>
12.2SEE	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.2SE</a>
12.2SEF	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.2SE</a>
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 <a href="#">リリース12.2EX</a>
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「 <a href="#">修正済みソフトウェアの取得</a> 」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「 <a href="#">修正済みソフトウェアの取得</a> 」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 <a href="#">リリース12.2SRD</a>
12.2SRB	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.2SRD</a>
12.2SRC	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.2SRD</a>
12.2SRD	脆弱性なし	12.2(33)SRD6
12.2SRE	脆弱性なし	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 <a href="#">リリース12.4</a>
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「 <a href="#">修正済みソフトウェアの取得</a> 」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 <a href="#">リリース12.2SXF</a>
12.2SXA	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.2SXF</a>
12.2SXB	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.2SXF</a>
12.2SXD	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.2SXF</a>
12.2SXE	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.2SXF</a>
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「 <a href="#">修正済みソフトウェアの取得</a> 」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「 <a href="#">修正済みソフトウェアの取得</a> 」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 <a href="#">リリース12.2SB</a>
12.2T	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.4</a>
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「 <a href="#">修正済みソフトウェアの取得</a> 」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 <a href="#">リリース12.4</a>
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	「 <a href="#">Cisco IOS-XEソフトウェアの可用性</a> 」を参照してください。	「 <a href="#">Cisco IOS-XEソフトウェアの可用性</a> 」を参照してください。
12.2XNB	「 <a href="#">Cisco IOS-XEソフトウェアの可用性</a> 」を参照してください。	「 <a href="#">Cisco IOS-XEソフトウェアの可用性</a> 」を参照してください。
12.2XNC	「 <a href="#">Cisco IOS-XEソフトウェアの可用性</a> 」	「 <a href="#">Cisco IOS-XEソフトウェアの可用性</a> 」を参照してください。

	を参照してください。	
12.2XND	「 <a href="#">Cisco IOS-XEソフトウェアの可用性</a> 」を参照してください。	「 <a href="#">Cisco IOS-XEソフトウェアの可用性</a> 」を参照してください。
12.2XNE	「 <a href="#">Cisco IOS-XEソフトウェアの可用性</a> 」を参照してください。	「 <a href="#">Cisco IOS-XEソフトウェアの可用性</a> 」を参照してください。
12.2XNF	「 <a href="#">Cisco IOS-XEソフトウェアの可用性</a> 」を参照してください。	「 <a href="#">Cisco IOS-XEソフトウェアの可用性</a> 」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 <a href="#">リリース12.4</a>
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「 <a href="#">修正済みソフトウェアの取得</a> 」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「 <a href="#">修正済みソフトウェアの取得</a> 」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「 <a href="#">修正済みソフトウェアの取得</a> 」セクションの手順に従って、サポート組

		<p>織にお問い合わせください。</p>
12.2YJ	脆弱性なし	<p>脆弱性が存在します。このアドバイザリの「<a href="#">修正済みソフトウェアの取得</a>」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。</p>
12.2YK	脆弱性なし	脆弱性なし
12.2YL	脆弱性なし	<p>脆弱性が存在します。このアドバイザリの「<a href="#">修正済みソフトウェアの取得</a>」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。</p>
12.2YM	脆弱性なし	<p>脆弱性あり。最初の修正は<a href="#">リリース12.4</a></p>
12.2YN	脆弱性なし	<p>脆弱性が存在します。このアドバイザリの「<a href="#">修正済みソフトウェアの取得</a>」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。</p>
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	<p>脆弱性が存在します。このアドバイザリの「<a href="#">修正済みソフトウェアの取得</a>」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。</p>

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「 <a href="#">修正済みソフトウェアの取得</a> 」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「 <a href="#">修正済みソフトウェアの取得</a> 」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「 <a href="#">修正済みソフトウェアの取得</a> 」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「 <a href="#">修正済みソフトウェアの取得</a> 」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「 <a href="#">修正済みソフトウェアの取得</a> 」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「 <a href="#">修正済みソフトウェアの取得</a> 」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。このアドバイザーの「 <a href="#">修正済みソフトウェアの取得</a> 」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。このアドバイザーの「 <a href="#">修正済みソフトウェアの取得</a> 」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。このアドバイザーの「 <a href="#">修正済みソフトウェアの取得</a> 」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 <a href="#">リリース12.2SXF</a>
12.2ZB	脆弱性なし	脆弱性が存在します。このアドバイザーの「 <a href="#">修正済みソフトウェアの取得</a> 」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 <a href="#">リリース12.4</a>
12.2ZF	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.4</a>

		<a href="#">リリース12.4</a>
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 <a href="#">リリース12.4</a>
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「 <a href="#">修正済みソフトウェアの取得</a> 」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 <a href="#">リリース12.2SXH</a>
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「 <a href="#">修正済みソフトウェアの取得</a> 」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「 <a href="#">修正済みソフトウェアの取得</a> 」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 )	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 12.3 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 )	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
--	---	--

12.4	脆弱性なし	12.4(25f)
12.4GC	12.4(24)GC4	12.4(24)GC4
12.4JA	脆弱性なし	脆弱性なし
12.4JAX	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
12.4JHA	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
12.4JMA	脆弱性なし	脆弱性なし
12.4JMB	脆弱性なし	脆弱性なし
12.4JX	脆弱性なし	脆弱性あり。12.4JAの任意のリリースに移行 12.4(21a)JXまでのリリースには脆弱性はありません。
12.4JY	脆弱性なし	脆弱性なし
12.4MD	脆弱性なし	12.4(24)MD6 ( 2011年10月28日 )
12.4MDA	脆弱性なし	12.4(24)MDA7
12.4MDB	脆弱性なし	12.4(24)MDB3
12.4MR	脆弱性なし	脆弱性が存在します。このアドバイザリの「 <a href="#">修正済みソフトウェアの取得</a> 」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	脆弱性なし	脆弱性が存在します。このアドバイザリの「 <a href="#">修正済みソフトウェアの取得</a> 」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	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リ</a>

		<a href="#">リリース12.4T</a>
12.4SW	脆弱性なし	脆弱性なし
12.4T	該当するのは 12.4(24)Tから 12.4(24)T4だ けです。最初 の修正は 12.4(24)T3cと 12.4(24)T5で す	12.4(24)T6 12.4(15)T16
12.4XA	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.4T</a>
12.4XB	脆弱性なし	12.4(2)XB12
12.4XC	脆弱性なし	脆弱性なし
12.4XD	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.4T</a>
12.4XE	脆弱性なし	脆弱性なし
12.4XF	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.4T</a>
12.4XG	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.4T</a>
12.4XJ	脆弱性なし	脆弱性なし



12.4XK	脆弱性なし	脆弱性なし
12.4XL	脆弱性なし	脆弱性が存在します。このアドバイザーの「 <a href="#">修正済みソフトウェアの取得</a> 」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 <a href="#">リリース12.4T</a>
12.4XN	脆弱性なし	脆弱性が存在します。このアドバイザーの「 <a href="#">修正済みソフトウェアの取得</a> 」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。このアドバイザーの「 <a href="#">修正済みソフトウェアの取得</a> 」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 <a href="#">リリース12.4T</a>
12.4XR	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.4T</a>
12.4XT	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.4T</a>
12.4XV	脆弱性なし	脆弱性なし

12.4XW	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.4T</a>
12.4XY	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.4T</a>
12.4XZ	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.4T</a>
12.4YA	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース12.4T</a>
12.4YB	脆弱性なし	脆弱性が存在します。このアドバイザーの「 <a href="#">修正済みソフトウェアの取得</a> 」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。このアドバイザーの「 <a href="#">修正済みソフトウェアの取得</a> 」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	脆弱性あり。2011年9月30日に12.4(22)YE6で修正済み。 2011年10月17日に12.4(24)YE7で入手可能
12.4YG	脆弱性なし	脆弱性が存在します。このアドバイザーの「 <a href="#">修正済みソフトウェアの取得</a> 」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 )	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)M5	15.0(1)M7
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「 <a href="#">修正済みソフトウェアの取得</a> 」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	脆弱性なし	脆弱性が存在します。このアドバイザリの「 <a href="#">修正済みソフトウェアの取得</a> 」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 : 「 <a href="#">Cisco IOS XEソフトウェアの可用性</a> 」を参照してください。	15.0(1)S4 Cisco IOS XEデバイス : 「 <a href="#">Cisco IOS XEソフトウェアの可用性</a> 」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「 <a href="#">修正済みソフトウェアの取得</a> 」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デバイス : 「 <a href="#">Cisco IOS XEソフトウェアの可用性</a> 」を参照してください。	Cisco IOS XEデバイス : 「 <a href="#">Cisco IOS XEソフトウェアの可用性</a> 」を参照してください。
15.0XA	脆弱性あり。最初の修正は <a href="#">リリース15.1T</a>	脆弱性あり。最初の修正は <a href="#">リリース15.1T</a>
15.0XO	Cisco IOS XEデバイス : 「 <a href="#">Cisco IOS XEソフトウェアの可用性</a> 」を参照してください。	Cisco IOS XEデバイス : 「 <a href="#">Cisco IOS XEソフトウェアの可用性</a> 」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 )	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「 <a href="#">修正済みソフトウェアの取得</a> 」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	脆弱性なし	脆弱性あり。最初の修正は <a href="#">リリース15.1T</a>
1,510万	脆弱性なし	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。このアドバイザーの「 <a href="#">修正済みソフトウェアの取得</a> 」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 : 「 <a href="#">Cisco IOS XEソフトウェアの可用性</a> 」を参照してください。	15.1(2)S2 15.1(3)S Cisco IOS XEデバイス : 「 <a href="#">Cisco IOS XEソフトウェアの可用性</a> 」を参照してください。
15.1T	15.1(1)T3 15.1(2)T3 15.1(3)T1	2011年12月9日の15.1(1)T4 15.1(2)T4 15.1(3)T2
15.1XB	脆弱性あり。 最初の修正は <a href="#">リリース15.1T</a>	脆弱性あり。最初の修正は <a href="#">リリース15.1T</a>
Affected 15.2- Based Releases	First Fixed Release ( 修正された最初のリリース )	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ーに対する最初の修正リリース
影響を受ける 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リリース	First Fixed Release ( 修正さ	2011年9月のバンドル公開に含まれるすべての
------------------	---------------------------	-------------------------

ス	れた最初のリリース)	アドバイザーに対する最初の修正リリース
2.1.x	脆弱性なし	脆弱性あり、3.3.2S以降に移行
2.2.x	脆弱性なし	脆弱性あり、3.3.2S以降に移行
2.3.x	脆弱性なし	脆弱性あり、3.3.2S以降に移行
2.4.x	脆弱性なし	脆弱性あり、3.3.2S以降に移行
2.5.x	脆弱性なし	脆弱性あり、3.3.2S以降に移行
2.6.x	脆弱性なし	脆弱性あり、3.3.2S以降に移行
3.1.xS	脆弱性なし	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	脆弱性なし	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	脆弱性なし	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』([http://www.cisco.com/en/US/docs/ios/ios\\_xe/2/release/notes/rnasr21.html#wp2310700](http://www.cisco.com/en/US/docs/ios/ios_xe/2/release/notes/rnasr21.html#wp2310700)、[http://www.cisco.com/en/US/docs/ios/ios\\_xe/3/release/notes/asr1k\\_rn\\_3s\\_sys\\_req.html#wp2999052](http://www.cisco.com/en/US/docs/ios/ios_xe/3/release/notes/asr1k_rn_3s_sys_req.html#wp2999052)、および[http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/release/note/OL\\_24726.html#wp2570252](http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/release/note/OL_24726.html#wp2570252))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、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

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。

## URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6>

## 改訂履歴

リビジョン 1.1	2011年 9月30日	IOSソフトウェアテーブルバンドル公開のアップデートの最初の修正済み情報。
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

本アドバイザー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。本アドバイザー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。

本アドバイザー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。