Cisco IOSソフトウェアのDHCPバージョン6サーバにおけるDoS脆弱性

High

アドバイザリーID : cisco-sa-20120926-dhcpv6
初公開日 : 2012-09-26 16:00
最終更新日 : 2012-10-18 19:01
バージョン 1.1 : Final
CVSSスコア : 7.1
回避策 : No Workarounds available
Cisco バグ ID : CSCto57723

CVE-2012-4623

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。攻撃者は、DHCPバージョン6(DHCPv6)サーバ機能が有効になっている該当デバイスに巧妙に細工された要求を送信することで、この脆弱性を不正利用し、リロードを引き起こす可能性があります。

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-20120926-dhcpv6

注：2012年9月26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。8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詳述された脆弱性を修正したCisco IOSソフトウェアリリースと、2012年9月のバンドル公開に含まれるすべての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: 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_sep12.html

該当製品

脆弱性のある製品

該当するCisco IOSソフトウェアまたはCisco IOS XEソフトウェアを実行し、DHCPv6サーバ機能が有効になっているシスコデバイスには脆弱性が存在します。DHCPv6サーバ機能は、デフォルトでは有効になっていません。 DHCPv6クライアントまたはリレーエージェントとして設定されているシスコデバイスは、この脆弱性の影響を受けません。

Cisco IOSデバイスまたはCisco IOS XEデバイスがDHCPv6サーバとして設定されているかどうかを確認するには、 show ipv6 dhcp interfaceコマンドを発行します。

次の例は、DHCPv6サーバとして設定されていないため、脆弱性が存在しないCisco IOSデバイスを示しています。

```
Router#show ipv6 dhcp interface
Router#
```

次の例は、この脆弱性の影響を受けるCisco IOSデバイスを示しています。DHCPv6サーバ機能がFastEthernet0/0インターフェイスに適用されているため、このデバイスには脆弱性が存在します。

```
Router#show ipv6 dhcp interface
FastEthernet0/0 is in server mode
  Using pool: DHCPv6-stateful
  Preference value: 0
  Hint from client: ignored
  Rapid-Commit: disabled
Router#
```

次の例は、この脆弱性の影響を受けるCisco IOSデバイスを示しています。DHCPv6サーバ機能がFastEthernet0/0およびFastEthernet0/1インターフェイスに適用されているため、このデバイスには脆弱性が存在します。

```
Router#show ipv6 dhcp interface | include server
FastEthernet0/0 is in server mode
FastEthernet0/1 is in server mode
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
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 XR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

Cisco IOSソフトウェアおよびCisco IOS XEソフトウェアのDHCPv6サーバ機能は、指定されたアドレスプールからDHCPv6クライアントにIPv6アドレス、プレフィックス、およびその他の情報を割り当てて管理するDHCPv6サーバ実装です。

Cisco IOSソフトウェアおよびCisco IOS XE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DoS状態を引き起こす可能性のある脆弱性が存在します。攻撃者は、DHCPv6サーバ機能が有効になっている該当デバイスに巧妙に細工された要求を送信することで、この脆弱性を不正利用し、リロードを引き起こす可能性があります。

この脆弱性は、該当するCisco IOSデバイスが不正なDHCPv6パケットの処理を試みたときに発生します。有効なDHCPv6パケット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。Cisco IOSデバイスが転送するDHCPv6パケット（たとえば、通過するDHCPv6トラフィック）は、この脆弱性を引き起こしません。

IPv4のDHCPサーバとして設定されているCisco IOSデバイスは、この脆弱性の影響を受けません。

この脆弱性は、Cisco Bug ID CSCto57723(登録ユーザ専用)として文書化されています。 この脆弱性には、Common Vulnerabilities and Exposures（CVE）ID として、CVE-2012-4623 が割り当てられています。

回避策

この脆弱性には回避策がありません

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 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。

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9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9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	脆弱性なし
12.2B	脆弱性なし	脆弱性あり。最初の修正はリリース12.4 12.2(4)B8までのリリースには脆弱性はありません。
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	12.2(15)BX 12.2(2)BX1までのリリースには脆弱性はありません。
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	脆弱性あり。12.2Sの任意のリリースに移行
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	脆弱性なし
12.2EWA	脆弱性なし	脆弱性なし
12.2EX	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	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。	はありません。
12.2EY	脆弱性あり。最初の修正はリリース 15.1EY 12.2(46)EY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 15.1EY 12.2(46)EYまでのリリースには脆弱性はありません。
12.2EZ	脆弱性なし	脆弱性なし
12.2FX	脆弱性なし	脆弱性なし
12.2FY	脆弱性なし	脆弱性なし
12.2FZ	脆弱性なし	脆弱性なし
12.2IRA	脆弱性あり。最初の修正はリリース 12.2SRE	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 12.2SRE	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 12.2SRE	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 12.2SRE	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 12.2SRE	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 12.2SRE	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	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。
12.2IRI	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。
12.2IXA	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	12.2(15)MC1までのリリースには脆弱性はありません。12.2(15)MC2b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12.4
12.2MRA	脆弱性あり。最初の修正はリリース12.2SRE	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	脆弱性なし
12.2SB	12.2(33)SB13	12.2(33)SB13
12.2SBC	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12.2SB
12.2SCA	脆弱性あり。最初の修正はリリース12.2SCF	脆弱性あり。最初の修正はリリース12.2SCF
12.2SCB	脆弱性あり。最初の修正はリリース12.2SCF	脆弱性あり。最初の修正はリリース12.2SCF
12.2SCC	脆弱性あり。最初の修正はリリース12.2SCF	脆弱性あり。最初の修正はリリース12.2SCF
12.2SCD	脆弱性あり。最初の修正はリリース12.2SCF	脆弱性あり。最初の修正はリリース12.2SCF
12.2SCE	脆弱性あり。最初の修正はリリース12.2SCF	脆弱性あり。最初の修正はリリース12.2SCF
12.2SCF	12.2(33)SCF4	12.2(33)SCF4
12.2SCG	脆弱性なし	脆弱性なし
12.2SE	12.2(46)SE1 12.2(55)SE6	12.2(46)SE1 12.2(55)SE6
12.2SEA	脆弱性なし	脆弱性なし
12.2SEB	脆弱性なし	脆弱性なし
12.2SEC	脆弱性なし	脆弱性なし
12.2SED	脆弱性なし	脆弱性なし
12.2SEE	脆弱性なし	脆弱性なし

12.2SEF	脆弱性なし	脆弱性なし
12.2SEG	脆弱性なし	脆弱性なし
12.2SG	12.2(53)SG8	12.2(53)SG8 脆弱性あり。12.2(46)SG1までのリリースには脆弱性はありません。
12.2SGA	脆弱性なし	脆弱性なし
12.2SM	脆弱性なし	脆弱性なし
12.2SO	脆弱性なし	脆弱性なし
12.2SQ	12.2(44)SQ2までのリリースには脆弱性はありません。	12.2(44)SQ2までのリリースには脆弱性はありません。
12.2SRA	脆弱性なし	脆弱性なし
12.2SRB	脆弱性なし	脆弱性なし
12.2SRC	脆弱性あり。最初の修正はリリース12.2SRE	脆弱性あり。最初の修正はリリース12.2SRE
12.2SRD	脆弱性あり。最初の修正はリリース12.2SRE	脆弱性あり。最初の修正はリリース12.2SRE
12.2SRE	12.2(33)SRE7	12.2(33)SRE7
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	脆弱性なし
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	脆弱性なし
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	脆弱性あり。12.2(33)SXH7までのリリースには脆弱性はありません。
12.2SXI	12.2(33)SXI10	12.2(33)SXI10
12.2日本語	12.2(33)SXJ4	12.2(33)SXJ4
12.2SY	12.2(50)SY3	12.2(50)SY3

	脆弱性が存在するのは、リリース 12.2(50)SYから12.2(50)SY2だけです。	
12.2SZ	脆弱性なし	脆弱性なし
12.2T	脆弱性なし	脆弱性あり。最初の修正はリリース12.4 12.2(8)T10までのリリースには脆弱性はありません。
12.2TPC	脆弱性なし	脆弱性なし
12.2WO	脆弱性あり。最初の修正はリリース 15.0SG	脆弱性あり。最初の修正はリリース 15.0SG
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	脆弱性あり。最初の修正はリリース 12.2SG 12.2(40)XO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 12.2SG 12.2(40)XOまで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	脆弱性なし
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12.4
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	脆弱性なし
12.2ZX	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12.2SB
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）	2012年9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	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.3B	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
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12.4	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12.4
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12.4 12.3(8)T11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12.4
12.3TPC	脆弱性なし	12.3(4)TPC11a までのリリースには脆弱性はありません。

12.3VA	脆弱性なし	脆弱性なし
12.3XA	脆弱性なし	12.3(2)XA7より前のリリースには脆弱性があり、12.3(2)XA7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12.4
12.3XB	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。
12.3XC	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.3XD	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.3XE	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
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12.4
12.3XI	脆弱性なし	12.3(7)XI1b
12.3XJ	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.3XK	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
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12.4T
12.3XQ	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.3XR	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.3XU	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T 12.3(8)XU1までのリリースには脆弱性はありません。
12.3XW	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.3XX	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.3XY	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
12.3XZ	脆弱性なし	脆弱性あり。最初の修正はリリース12.4
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12.4T
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12.4T
12.3YG	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

	12.4T	12.4T
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 12.4T
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 12.4T
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 12.4T
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 12.4T
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 12.4T
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 12.4T
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 12.4T
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 12.4T
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 12.4T
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	脆弱性なし	脆弱性あり。最初の修正はリリース 12.4T
Affected 12.4-Based Releases	First Fixed Release（修正された最初のリリース）	2012年9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)	12.4(25g)
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
12.4JAX	脆弱性なし	脆弱性なし
12.4ジェイ	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	12.4(24)MD7
12.4MDA	脆弱性あり。12.4MDの任意のリリースに移行 12.4(22)MDA6までのリリースには脆弱性はありません。	12.4(22)MDA6までのリリースには脆弱性はありません
12.4MDB	12.4(24)MDB10	12.4(24)MDB10
12.4MR	12.4(16)MR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12.4T	脆弱性あり。最初の修正はリリース12.4T
12.4SW	脆弱性なし	脆弱性なし
12.4T	12.4(24)T8	12.4(24)T8
12.4XA	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
12.4XB	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12.4T
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12.4T
12.4XE	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

	12.4T	12.4T
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 12.4T
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 12.4T
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 12.4T
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 12.4T
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	12.4(15)XMまでのリリースには脆弱性はありません。 12.4(15)XM3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 12.4T	12.4(15)XMまでのリリースには脆弱性はありません。12.4(15)XM3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12.4T
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。
12.4XQ	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 12.4T
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 12.4T
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 12.4T
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 12.4T

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 12.4T
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 12.4T
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	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
12.4YG	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）	2012年9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
15.0EX	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)M9	15.0(1)M9
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)S6 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)S6 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	15.0(2)SE	15.0(2)SE

15.0SG	15.0(2)SG5 15.0(2)SG6（2012年10月11日に入手可能） 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)SG5 15.0(2)SG6（2012年10月11日に入手可能） 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)SY2	15.0(1)SY2
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）	2012年9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)EY4	15.1(2)EY4
15.1GC	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
1,510万	15.1(4)M5	15.1(4)M5
15.1MR	15.1(3)MR（2012年10月1日に入手可能）	15.1(3)MR（2012年10月1日に入手可能）
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。	15.1(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。
15.1SG	15.1(1)SG1 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(1)SG1 15.1(2)SG 12-NOV-12 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	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。	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	脆弱性あり。15.2SNGの任意のリリースに移行	脆弱性あり。15.2SNGの任意のリリースに移行
15.1SV	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。
15.1T	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）	2012年9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(3)GCより前のリリースには脆弱性があり、15.2(3)GC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15.2T	15.2(3)GCより前のリリースには脆弱性があり、15.2(3)GC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15.2T
15.2JA	脆弱性なし	脆弱性なし
1,520万	15.2(4)M	脆弱性なし
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(1)S2 15.2(2)S1 15.2(4)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。
15.2SNG	脆弱性なし	脆弱性なし
15.2T	15.2(1)T3 15.2(2)T2 15.2(3)T2（10月12日に入手可能）	15.2(1)T3 15.2(2)T2 15.2(3)T2（10月12日に入手可能）

Cisco IOS XE ソフトウェア

Cisco IOS XEソフトウェアは、この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9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。3.4.0S以降に移行してください。	脆弱性あり。3.6.0S以降に移行してください。
2.2.x	脆弱性あり。3.4.0S以降に移行してください。	脆弱性あり。3.6.0S以降に移行してください。
2.3.x	脆弱性あり。3.4.0S以降に移行してください。	脆弱性あり。3.6.0S以降に移行してください。
2.4.x	脆弱性あり。3.4.0S以降に移行してください。	脆弱性あり。3.6.0S以降に移行してください。
2.5.x	脆弱性あり。3.4.0S以降に移行してください。	脆弱性あり。3.6.0S以降に移行してください。
2.6.x	脆弱性あり。3.4.0S以降に移行してください。	脆弱性あり。3.6.0S以降に移行してください。
3.1.xS	3.1.4S	3.1.4S
3.1.xSG	脆弱性あり。3.2.5SG以降に移行してください。	脆弱性あり。3.2.5SG以降に移行してください。
3.2.xS	脆弱性あり。	脆弱性あり。3.6.0S以降

	3.4.0S以降に移行してください。	に移行してください。
3.2.xSG	3.2.5SG	3.2.5SG
3.2.xXO	脆弱性あり、3.3.1SG以降に移行	脆弱性あり。3.3.1SG以降に移行してください。
3.3.xS	脆弱性あり。3.4.0S以降に移行してください。	脆弱性あり。3.6.0S以降に移行してください。
3.3.x.SG	3.3.1SG	3.3.1SG
3.4.xS	脆弱性なし	脆弱性あり。3.6.0S以降に移行してください。
3.5.xS	脆弱性なし	脆弱性あり。3.6.0S以降に移行してください。
3.6.xS	脆弱性なし	脆弱性なし
3.7.xS	脆弱性なし	脆弱性なし

Cisco IOS XR ソフトウェア

Cisco IOS XRソフトウェアは、この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、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-20120926-dhcpv6

改訂履歴

リビジョン 1.1	2012年 10月18日	Cisco IOS 12.2(46)SE1を追加の初回修正リリースとして追加。
リビジョン 1.0	2012年9月 26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。