Cisco IOSソフトウェアのDHCPにおけるDoS脆弱性

アドバイザリーID : cisco-sa-20130925-dhcp
初公開日 : 2013-09-25 16:00
バージョン 1.0 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID : CSCug31561

CVE-2013-5475

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DHCP実装における脆弱性により、認証されていないリモート攻撃者がサービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、巧妙に細工されたDHCPパケットの解析中に発生します。攻撃者は、DHCPサーバまたはDHCPリレー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DHCP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。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。

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-20130925-dhcp

注：2013年9月25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8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: 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_sep13.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、DHCPサーバまたはDHCPリレー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。DHCPサーバまたはDHCPリレー機能は、デフォルトでは有効になっていません。DHCPクライア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DHCP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 ip dhcp poolコマンドを発行します。

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。このデバイスは、DHCPサーバ機能が有効になっており、設定されたプールにIPアドレスを提供するサブネットが少なくとも1つあるため、脆弱です。

```
<#root>

Router#show ip dhcp pool

Pool test

 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses

 192.168.1.1          192.168.1.1      - 192.168.1.254         0
```

Cisco IOSデバイスまたはCisco IOS XEデバイスがDHCPリレーエージェントとして設定されているかどうかを確認するには、 show run | include helper-addressコマンドを使用します。

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。このデバイスは、ip helper-addressの出力に基づいてDHCPリレーエージェント機能が有効になっているため、脆弱性の影響を受けます。

```
Router#show run | include helper-address
 ip helper-address 10.1.1.2
```

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DHCPサーバ機能は、指定されたアドレスプールからDHCPクライアントにIPバージョン4(IPv4)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DHCPサーバ実装です。
Cisco IOSソフトウェアおよびCisco IOS XEソフトウェアのDHCPリレーエージェント機能は、クライアントとサーバ間でDHCPパケットを転送します。リレーエージェントは、クライアントとサーバが同じ物理サブネット上にない場合に、それらの間で要求と応答を転送するために使用されます。

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、DHCPサーバまたはDHCPリレーエージェント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デバイスが巧妙に細工されたDHCPパケットを処理しようとするときに発生します。有効なDHCPパケットでは、この脆弱性は引き起こされません。Cisco IOSデバイスが転送するDHCPパケット（通過するDHCPトラフィックなど）はこの脆弱性を引き起こしませんが、DHCPリレーエージェントに転送されるパケットはこの脆弱性を引き起こします。

IPバージョン6(IPv6)のDHCPバージョン6(DHCPv6)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 CSCug31561(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-2013-5475 が割り当てられています。

回避策

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

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。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）	2013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
12.2EX	脆弱性あり。最初の修正はリリース15.0SE	脆弱性あり。最初の修正はリリース15.0SE
12.2EY	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
12.2EZ	12.2(60)EZ	12.2(60)EZ2より前のリリースには脆弱性があり、12.2(60)EZ2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
12.2IRB	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」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」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」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。
12.2IXG	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」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。
12.2IXH	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」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。
12.2MC	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

	15.1M	15.1M
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」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。
12.2SB	12.2(33)SB15	12.2(33)SB15
12.2SCA	脆弱性あり。最初の修正はリリース 12.2SCH	脆弱性あり。最初の修正はリリース 12.2SCH
12.2SCB	脆弱性あり。最初の修正はリリース 12.2SCH	脆弱性あり。最初の修正はリリース 12.2SCH
12.2SCC	脆弱性あり。最初の修正はリリース 12.2SCH	脆弱性あり。最初の修正はリリース 12.2SCH
12.2SCD	脆弱性あり。最初の修正はリリース 12.2SCH	脆弱性あり。最初の修正はリリース 12.2SCH
12.2SCE	脆弱性あり。最初の修正はリリース 12.2SCH	脆弱性あり。最初の修正はリリース 12.2SCH
12.2SCF	脆弱性あり。最初の修正はリリース 12.2SCH	脆弱性あり。最初の修正はリリース 12.2SCH
12.2SCG	脆弱性あり。最初の修正はリリース 12.2SCH	脆弱性あり。最初の修正はリリース 12.2SCH
12.2SCH	12.2(33)SCH1	12.2(33)SCH1
12.2SE	12.2(55)SE8	12.2(55)SE8
12.2SEG	脆弱性あり。最初の修正はリリース 15.0SE	脆弱性あり。最初の修正はリリース 15.0SE
12.2SG	12.2(53)SG10(2013年12月に入手可能)*	12.2(53)SG10(2013年12月に入手可能)*
12.2SGA	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」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。
12.2SM	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」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。
12.2SQ	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」の手順に従って、サポート組織にお問	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

	い合わせください。	お問い合わせください。
12.2SRA	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
12.2SRB	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
12.2SRC	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)SRE9	12.2(33)SRE9
12.2STE	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」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。
12.2SV	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」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。
12.2SVD	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」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。
12.2SVE	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」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。
12.2SW	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
12.2SXF	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」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。
12.2SXH	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」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。
12.2SXI	12.2(33)SXI12	12.2(33)SXI12
12.2日本語	12.2(33)SXJ6	12.2(33)SXJ6
12.2SY	脆弱性あり。最初の修正はリリース 15.0SY	脆弱性あり。最初の修正はリリース 15.0SY

12.2WO	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」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。
12.2XNA	「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」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。
12.2ZYA	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」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。
Affected 12.3-Based Releases	First Fixed Release（修正された最初のリリース）	2013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
12.3BC	脆弱性あり。最初の修正はリリース12.2SCH	脆弱性あり。最初の修正はリリース12.2SCH
12.3JEC	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」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。
12.3JED	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」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。
12.3JEE	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

12.3JX	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
12.3XI	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
12.3XJ	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
12.3XK	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
12.3XL	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
12.3XQ	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
12.3XR	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
12.3XU	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
12.3XW	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
12.3XX	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
12.3YD	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
12.3YF	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
12.3YG	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
12.3YI	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
12.3YJ	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
12.3YK	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
12.3YM	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
12.3YQ	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
12.3YS	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
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

	15.1M	15.1M
12.3YU	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
12.3YX	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
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」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 15.1M	脆弱性あり。最初の修正はリリース 15.1M
Affected 12.4-Based Releases	First Fixed Release（修正された最初のリリース）	2013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	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
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」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
12.4JAL	脆弱性あり。最初の修正はリリース 12.4JAM	脆弱性あり。最初の修正はリリース 12.4JAM
12.4ジャム	12.4(25e)JAM2	12.4(25e)JAM2
12.4JAN	脆弱性なし	脆弱性なし
12.4JAX	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
12.4JAZ	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」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。
12.4JDA	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」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。
12.4JDC	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」の手順に従って、サポート組織にお問	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

	い合わせください。	お問い合わせください。
12.4JDD	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」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。
12.4JDE	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
12.4JHA	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」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。
12.4JHB	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」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。
12.4JHC	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
12.4JK	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」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。
12.4JL	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」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。
12.4JX	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
12.4JY	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
12.4JZ	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
12.4MD	脆弱性あり。最初の修正はリリース 12.4MDB	脆弱性あり。最初の修正はリリース 12.4MDB
12.4MDA	脆弱性あり。最初の修正はリリース 12.4MDB	脆弱性あり。最初の修正はリリース 12.4MDB
12.4MDB	12.4(24)MDB15	12.4(24)MDB15
12.4MR	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」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。

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」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15.1M	脆弱性あり。最初の修正はリリース15.1M
12.4SW	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
12.4T	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
12.4XA	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
12.4XB	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
12.4XC	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
12.4XD	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
12.4XE	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
12.4XF	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
12.4XG	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
12.4XJ	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
12.4XK	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
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」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	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
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」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	脆弱性が存在します。このアドバイザリ

	リの「修正済みソフトウェアの取得」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。
12.4XQ	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
12.4XR	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
12.4XT	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
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」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 15.1M	脆弱性あり。最初の修正はリリース 15.1M
12.4XY	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
12.4XZ	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
12.4YA	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
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」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」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 15.1M	脆弱性あり。最初の修正はリリース 15.1M
12.4YG	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」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。
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
15.0EA	15.0(2)EA1	15.0(2)EA1

15.0EB	脆弱性あり。15.2Eの任意のリリースに移行	脆弱性あり。15.2Eの任意のリリースに移行
15.0EC	脆弱性あり。15.2Eの任意のリリースに移行	脆弱性あり。15.2Eの任意のリリースに移行
15.0ED	注：15.0(2)ED1より前のリリースには脆弱性があり、15.0(2)ED1以降のリリースには脆弱性はありません。	注：15.0(2)ED1より前のリリースには脆弱性があり、15.0(2)ED1以降のリリースには脆弱性はありません。
15.0EH	脆弱性なし	脆弱性なし
15.0EJ	脆弱性なし	脆弱性なし
15.0EX	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。
15.0EY	15.0(2)EY2	15.0(2)EY2
15.0EZ	脆弱性が存在するのは、リリース15.0(2)EZだけです	脆弱性が存在するのは、リリース15.0(2)EZだけです
15.0M	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
15.0MR	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」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	15.0(2)SE4	15.0(2)SE4
15.0SG	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」の手順に従って、サポート組織にお問い合わせください。 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。	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。 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。

15.0SQB	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	15.0(1)SY5	15.0(1)SY5
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	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」の手順に従って、サポート組織にお問い合わせください。 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。	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。 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	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)M7	15.1(4)M7
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」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	15.1(3)MRA2	15.1(3)MRA2
15.1S	15.1(3)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。	15.1(3)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。
15.1SG	15.1(2)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(2)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。
15.1SNG	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」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」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」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。
15.1SVD	脆弱性なし	脆弱性なし
15.1SVE	脆弱性なし	脆弱性なし
15.1SVF	脆弱性なし	脆弱性なし
15.1SY	15.1(1)SY2（2013年10月28日に入手可能） 15.1(2)SY 15.1(2)SY1（2013年12月13日に入手可能）	15.1(1)SY2（2013年10月28日に入手可能） 15.1(2)SY
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
15.1XO	脆弱性なし	脆弱性なし
Affected 15.2-Based Releases	First Fixed Release（修正された最初のリリース）	2013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
15.2E	脆弱性なし	脆弱性なし
15.2GC	15.2(4)GC	脆弱性あり。15.4Tの任意のリリースに移行
15.2JA	15.2(4)JA1	15.2(4)JA1
15.2JAX	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」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。
15.2JB	15.2(2)JB2	15.2(2)JB2
15.2JN	脆弱性なし	脆弱性なし
1,520万	15.2(4)M4	15.2(4)M4
15.2秒	15.2(4)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。	15.2(4)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。

15.2SA	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」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」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	脆弱性あり。最初の修正はリリース15.3S	脆弱性あり。最初の修正はリリース15.3S
15.2T	15.2(2)T4 15.2(3)T4	15.2(3)T4
Affected 15.3-Based Releases	First Fixed Release（修正された最初のリリース）	2013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
1,530万	脆弱性なし	脆弱性なし
15.3秒	15.3(2)S2 15.3(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。	15.3(2)S2 15.3(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。
15.3T	15.3(1)T2 15.3(2)T1	15.3(1)T2 15.3(2)T1

* Cisco Catalyst 4500 Supervisor Engines 6-Eまたは6L-Eを搭載したCisco Catalyst 4500シリーズスイッチは、 Cisco IOSソフトウェアリリース15.1SGに移行できます。

Cisco IOS XE ソフトウェア

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 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）	2013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。3.4.6S以降に移行してください。	脆弱性あり。3.4.6S以降に移行してください。
2.2.x	脆弱性あり。3.4.6S以降に移行してください。	脆弱性あり。3.4.6S以降に移行してください。
2.3.x	脆弱性あり。3.4.6S以降に移行してください。	脆弱性あり。3.4.6S以降に移行してください。
2.4.x	脆弱性あり。3.4.6S以降に移行してください。	脆弱性あり。3.4.6S以降に移行してください。
2.5.x	脆弱性あり。3.4.6S以降に移行してください。	脆弱性あり。3.4.6S以降に移行してください。
2.6.x	脆弱性あり。3.4.6S以降に移行してください。	脆弱性あり。3.4.6S以降に移行してください。
3.1.xS	脆弱性あり。3.4.6S以降に移行してください。	脆弱性あり。3.4.6S以降に移行してください。
3.1.xSG	脆弱性あり。3.4.1SG以降に移行してください。	脆弱性あり。3.4.1SG以降に移行してください。
3.2.xS	脆弱性あり。3.4.6S以降に移行してください。	脆弱性あり。3.4.6S以降に移行してください。
3.2.xSE	3.2.3SE	3.2.3SE

3.2.xSG	脆弱性あり。3.4.1SG以降に移行してください。	脆弱性あり。3.4.1SG以降に移行してください。
3.2.xXO	脆弱性あり、3.3.0XO以降に移行	脆弱性あり。3.3.0XO以降に移行してください。
3.2.xSQ	脆弱性なし	脆弱性あり。3.3.0SQ以降に移行してください。
3.3.xS	脆弱性あり。3.4.6S以降に移行してください。	脆弱性あり。3.4.6S以降に移行してください。
3.3xSG	脆弱性あり。3.4.1SG以降に移行してください。	脆弱性あり。3.4.1SG以降に移行してください。
3.3xXO	脆弱性なし	脆弱性なし
3.3 X平方	脆弱性なし	脆弱性なし
3.4.xS	3.4.6S	3.4.6S
3.4.xSG	3.4.1SG*	3.4.1SG*
3.5.xE	脆弱性なし	脆弱性なし
3.5.xS	脆弱性あり。3.7.4S以降に移行してください。	脆弱性あり。3.7.4S以降に移行してください。
3.5.xE	脆弱性なし	脆弱性なし
3.6.xS	脆弱性あり。3.7.4S以降に移行してください。	脆弱性あり。3.7.4S以降に移行してください。
3.7.xS	3.7.2tS	3.7.4S
3.8.xS	3.9.2S	脆弱性あり。3.9.2S以降に移行してください。
3.9.xS	3.9.2S	3.9.2S
3.10.xS	脆弱性なし	脆弱性なし

* Cisco Catalyst 4500 Supervisor Engines 7-Eおよび7L-Eを搭載したCisco Catalyst 4500シリーズスイッチ、およびCisco Catalyst 4500-Xシリーズスイッチは、 Cisco IOS XEソフトウェアリリース3.4SGに移行できます。

Cisco IOS XR ソフトウェア

Cisco IOS XRソフトウェアは、2013年9月のCisco IOS Software Security Advisory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 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、該当製品の社内セキュリティレビューで発見されたものです。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-dhcp

改訂履歴

リビジョン 1.0	2013年9月25日	初版リリース

利用規約

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。