Cisco IOSソフトウェアのネットワークアドレス変換の脆弱性

アドバイザリーID : cisco-sa-20120926-nat
初公開日 : 2012-09-26 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 : CSCtr46123 CSCtn76183

CVE-2012-4619
CVE-2012-4618

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ソフトウェアのネットワークアドレス変換(NAT)機能には、IPパケットの変換における2つのサービス拒否(DoS)の脆弱性が存在します。

脆弱性のあるデバイスで転送中のパケットに変換が必要になると、この脆弱性が発生します。

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-nat

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

Cisco IOSソフトウェアを実行しているシスコデバイスは、NATが設定されている場合に脆弱性の影響を受けます。脆弱性の1つに、リリースに含まれるSession Initiation Protocol(SIP)のNATのサポートが必要です。
デバイスにNATが設定されているかどうかを確認するには、次の2つの方法があります。

- 実行中のデバイスでNATがアクティブかどうかを確認します。
- デバイスの設定にNATコマンドが含まれているかどうかを確認します。

実行中のデバイスでNATがアクティブかどうかの確認

Cisco IOSデバイスでNATが有効になっ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 ip nat statisticsコマンドを発行することを推奨します。NATがアクティブな場合、Outside interfacesとInside interfacesのセクションにはそれぞれ少なくとも1つのインターフェイスが含まれます。次の例は、NAT機能がアクティブになっているデバイスを示しています。

```
<#root>

Router#

show ip nat statistics


Total translations: 2 (0 static, 2 dynamic; 0 extended)

Outside interfaces: Serial0
Inside interfaces: Ethernet1

Hits: 135  Misses: 5
Expired translations: 2
Dynamic mappings:
-- Inside Source
access-list 1 pool mypool refcount 2
 pool mypool: netmask 255.255.255.0
        start 192.168.10.1 end 192.168.10.254
        type generic, total addresses 14, allocated 2 (14%), misses 0
```

Cisco IOSソフトウェアリリースによっては、Outside interfacesとInside interfacesの後に続く行にインターフェイスリストが表示される場合があります。showコマンドのsectionフィルタをサポートしているリリースでは、管理者はshow ip nat statistics | section interfacesコマンドを使用します。次に例を示します。

```
<#root>
```

```
Router>

show ip nat statistics | section interfaces

Outside interfaces:
  GigabitEthernet0/0
Inside interfaces:
  GigabitEthernet0/1
Router>
```

デバイスの設定にNATコマンドが含まれているか確認する

また、Cisco IOSソフトウェアの設定でNATが有効になっているかどうかを判断するには、ip nat insideコマンドまたはip nat outsideコマンドが異なるインターフェイスにあるか、NAT仮想インターフェイスの場合はip nat enableインターフェイスコマンドが存在する必要があります。show configuration | include ip natコマンドを使用すると、次の例に示すように、設定にNATが存在するかどうかを確認できます。

<#root>

```
Router>

show configuration | include ip nat

 ip nat inside
 ip nat outside
Router>
```

<#root>

```
Router>

show configuration | include ip nat

 ip nat enable
Router>
```

Cisco IOSソフトウェアリリースの判別

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

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ソフトウェアのSIP向けNATにおけるDoS脆弱性

NAT SIP Application Layer Gateway(ALG)機能は、IPパケットのSIPペイロードに埋め込まれたIPアドレスを変換することで、SIPに基づいてVoIPソリューション間にCisco IOS NATを導入する機能を追加します。
Cisco IOSソフトウェアには、SIPパケットのNAT処理に関する脆弱性が存在します。この脆弱性は、NAT SIP ALG機能が有効な場合に存在します。

NAT SIP ALGはデフォルトで有効になっており、IPパケットのSIPペイロード変換を実行します。 NAT SIP変換は、デフォルトではUDPポート5060パケットで実行されます。ポートは、 ip nat service sip udp port グローバルコンフィギュレーションコマンドを使用して設定できます。

この脆弱性は、Cisco Bug ID CSCtn76183(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-2012-4618が割り当てられています

Cisco IOSソフトウェアのNATにおけるDoS脆弱性

IP NAT機能は、ネットワーク間を移動するパケットのIPアドレスを宛先ネットワークで有効になるように変換する必要がある場合に、ネットワークの相互接続を可能にします。
Cisco IOSソフトウェアには、IPパケットのNAT処理に関する脆弱性が存在します。この脆弱性が不正利用されると、DoS状態が発生します。

この脆弱性は、Cisco Bug ID CSCtr46123(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2012-4619が割り当てられています

回避策

Cisco IOSソフトウェアのSIP向けNATにおけるDoS脆弱性

この脆弱性は、 no ip nat service sip udp port 5060グローバルコンフィギュレーションコマンドを使用してNAT SIP ALG over UDPトランスポートを無効にすることで緩和できます。このコマンドは、NAT ALG SIP機能を含むCisco IOSイメージでのみ設定できます。レイヤ3 NAT変換はSIPパケットに対して引き続き実行されますが、SIPペイロードは変換されません。

Cisco IOSソフトウェアのNATにおけるDoS脆弱性

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

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	脆弱性なし	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。
12.2EY	脆弱性なし	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	脆弱性なし	脆弱性あり。最初の修正はリリース 12.2SRE
12.2IRB	脆弱性なし	脆弱性あり。最初の修正はリリース 12.2SRE
12.2IRC	脆弱性なし	脆弱性あり。最初の修正はリリース 12.2SRE
12.2IRD	脆弱性なし	脆弱性あり。最初の修正はリリース 12.2SRE
12.2IRE	脆弱性なし	脆弱性あり。最初の修正はリリース 12.2SRE
12.2IRF	脆弱性なし	脆弱性あり。最初の修正はリリース 12.2SRE
12.2IRG	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。
12.2IRH	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。
12.2IRI	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。
12.2IXA	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	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRE
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	脆弱性なし
12.2SB	脆弱性なし	12.2(33)SB13
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12.2SCF
12.2SCB	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SCF
12.2SCC	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SCF
12.2SCD	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SCF
12.2SCE	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SCF
12.2SCF	脆弱性なし	12.2(33)SCF4
12.2SCG	脆弱性なし	脆弱性なし
12.2SE	脆弱性なし	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	脆弱性なし	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	脆弱性なし	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	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRE
12.2SRD	脆弱性なし	脆弱性あり。最初の修正はリリース12.2SRE
12.2SRE	脆弱性なし	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	脆弱性あり。12.2(33)SXH7までのリリースには脆弱性はありません。	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)SXI7 12.2(33)SXI4bまでの脆弱性はありません。	12.2(33)SXI10
12.2日本語	12.2(33)SXJ1	12.2(33)SXJ4
12.2SY	12.2(50)SY3 12.2(50)SYから12.2(50)SY2までにのみ脆弱	12.2(50)SY3

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	脆弱性なし	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	脆弱性なし	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	脆弱性なし	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
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）	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) ～からのみ脆弱である 12.4(23a) ～ 12.4(25f)	12.4(25g)
12.4GC	12.4(22)GC1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。
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	12.4(24)MD7	12.4(24)MD7
12.4MDA	脆弱性が存在します。脆弱性が存在するのは、リリース12.4(24)MDA1 ～ 12.4(24)MDA10だけです。	脆弱性あり。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	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。
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「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	脆弱性なし	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	脆弱性が存在します。脆弱性が存在するのは、リリース12.4(15)T13 ～ 12.4(24)T6だけです。	12.4(24)T8
12.4XA	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4XB	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4XC	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4XD	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4XE	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4XF	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4XG	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4XJ	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4XK	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
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	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12.4T
12.4XR	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4XT	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4XV	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。
12.4XW	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4XY	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4XZ	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4YA	脆弱性なし	脆弱性あり。最初の修正はリリース12.4T
12.4YB	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。
12.4YD	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	脆弱性あり。最初の修正はリリース12.4T 12.4(22)YE6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12.4T
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」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。
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)M8	15.0(1)M9
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。
15.0MRA	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。	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	脆弱性なし	15.0(2)SE
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。	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	脆弱性なし	15.0(1)SY2
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15.1M
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	脆弱性なし	15.1(2)EY4
15.1GC	15.1(2)GC2	脆弱性あり。最初の修正はリリース15.1M
1,510万	15.1(4)M3	15.1(4)M5

15.1MR	脆弱性なし	15.1(3)MR（2012年10月1日に入手可能）
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)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	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(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	15.1(2)T5 15.1(3)T3	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15.1T	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(2)GC	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	脆弱性なし	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)T1 15.2(3)T	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、TACサービスリクエストのトラブルシューティング中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-nat

改訂履歴

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

本アドバイザリ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。 本アドバイザリ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。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、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。