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-20130327-nat CVE-2013-1142
初公開日 : 2013-03-27 16:00
最終更新日 : 2013-04-11 17:17
バージョン 1.3 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID : CSCtz96745 CSCtg47129

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

Virtual Routing and Forwarding(VRF)対応のネットワークアドレス変換(NAT)機能のCisco IOSソフトウェア実装には、IPパケットの変換時に脆弱性が存在するため、認証されていないリモートの攻撃者によってサービス妨害(DoS)状態が引き起こされる可能性があります。

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。これらの脆弱性に対しては回避策がありません。

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-20130327-nat

注：2013年3月27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7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3月のバンドル公開のすべての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_mar13.html

該当製品

この脆弱性は、該当するバージョンのCisco IOSソフトウェアを実行し、VRF対応NAT設定を持つデバイスに影響を与えます。

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、VRF対応NATが設定されている場合に脆弱性の影響を受けます。

デバイスでVRF対応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。

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

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、デバイス設定を調べて、VRF対応のNATコマンドが含まれているかどうかを確認することをお勧めします。

デバイスの設定にVRF対応NATコマンドが含まれているかどうかの確認

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確認するには、少なくとも1つのip natグローバルコンフィギュレーションコマンドにvrfキーワードが含まれている必要があります。show configuration | include ip nat .* vrf .*コマンドを使用すると、次の例に示すように、VRF対応NATが設定に存在するかどうかを確認できます。

```
<#root>

Router>

show running-config | include ip nat .* vrf .*

ip nat inside source static 192.168.121.113 2.2.2.1 vrf VRF-Red
Router>
```

デバイスでVRF対応NATがアクティブかどうかの確認

管理者は、NAT機能とVRF機能の両方がアクティブであることを確認することで、Cisco IOSデバイスでVRF対応NATが有効になっているかどうかを確認できます。

アクティブなNAT機能のチェック

最初に、show ip nat statisticsコマンドを入力します。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および Inside interfacesの行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>
```

アクティブなVRF機能のチェック

脆弱な状態の2番目の要件は、少なくとも1つのインターフェイスでVRFがアクティブであることです。この場合、次の例に示すように、show ip vrfコマンドにはインターフェイス名が付いた行が少なくとも1つ含まれます。

```
<#root>

Router>

show ip vrf

  Name                              Default RD          Interfaces
  Red-VRF                           1:1                 Gi0/1
```

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

VRF対応NAT機能が設定されていないCisco IOSデバイスは脆弱ではありません。

次の製品には脆弱性が存在しないことが確認されています。

- Cisco IOS XE ソフトウェア
- Cisco IOS XR ソフトウェア
- Cisco NX-OS ソフトウェア
- Cisco ASA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

Cisco IOSソフトウェアのVRF対応NAT実装には脆弱性があり、認証されていないリモートの攻撃者がメモリ枯渇状態を引き起こす可能性があります。この脆弱性の問題は、競合状態の不適切な処理により、該当デバイスで使用可能なメモリが減少することに起因します。攻撃者がこの脆弱性を繰り返し不正利用し、DoS状態を引き起こす可能性があります。この脆弱性は、IPバージョン4(IPv4)パケットを使用して不正利用される可能性があります。この脆弱性を不正利用するためにTCP 3ウェイハンドシェイクは必要ありません。

この脆弱性は、Cisco Bug ID CSCtg47129(登録ユーザ専用)およびCSCtz96745(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-2013-1142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 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。2013年3月のFirst Fixed Release for All Advisories Bundled Publication列には、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で公開されたすべての脆弱性を修正する最初の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3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 12.2-Based Releases	First Fixed Release（修正された最初のリリース）	2013年3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	脆弱性なし
12.2B	脆弱性なし	脆弱性なし
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	脆弱性なし
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	脆弱性なし
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	脆弱性あり。最初の修正はリリース 12.2SG 12.2(20)EW4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(20)EW4までのリリースには脆弱性はありません。
12.2EWA	脆弱性あり。最初の修正はリリース 12.2SG 12.2(20)EWA4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(20)EWA4までのリリースには脆弱性はありません。
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

	12.2(37)EX までのリリースには脆弱性はありません。	12.2(37)EX までのリリースには脆弱性はありません。
12.2EY	12.2(58)EYより前のリリースには脆弱性があり、12.2(58)EY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15.1EY	脆弱性あり。最初の修正はリリース15.2S
12.2EZ	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
12.2FX	脆弱性あり。最初の修正はリリース12.2SE	脆弱性あり。最初の修正はリリース15.0SE
12.2FY	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
12.2FZ	脆弱性あり。最初の修正はリリース12.2SE	脆弱性あり。最初の修正はリリース15.0SE
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	脆弱性なし
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	Vulnerable.12.2(25)S15全体のリリース12.2(25)Sにのみ脆弱性があります。	Vulnerable.脆弱性が存在するのは、リリース12.2(25)S ~ 12.2(25)S15だけです
12.2SB	12.2(33)SB12	12.2(33)SB12
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
12.2SCH	脆弱性なし	脆弱性なし
12.2SE	脆弱性なし	12.2(55)SE7 12.2(54)SE4までのリリースには脆弱性

		はありません。
12.2SEA	脆弱性あり。最初の修正はリリース 12.2SE	脆弱性あり。最初の修正はリリース 15.0SE
12.2SEB	脆弱性あり。最初の修正はリリース 12.2SE	脆弱性あり。最初の修正はリリース 15.0SE
12.2SEC	脆弱性あり。最初の修正はリリース 12.2SE	脆弱性あり。最初の修正はリリース 15.0SE
12.2SED	脆弱性あり。最初の修正はリリース 12.2SE	脆弱性あり。最初の修正はリリース 15.0SE
12.2SEE	脆弱性あり。最初の修正はリリース 12.2SE	脆弱性あり。最初の修正はリリース 15.0SE
12.2SEF	脆弱性あり。最初の修正はリリース 12.2SE	脆弱性あり。最初の修正はリリース 15.0SE
12.2SEG	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15.0SE	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15.0SE
12.2SG	12.2(53)SG8	12.2(53)SG9
12.2SGA	脆弱性あり。最初の修正はリリース 12.2SG	脆弱性あり。最初の修正はリリース 12.2SG
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」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。
12.2SO	脆弱性なし	脆弱性なし
12.2SQ	12.2(50)SQ5	12.2(50)SQ5
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)SRE6 ‡	12.2(33)SRE8
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	Vulnerable.脆弱性が存在するのは、リリ	

	ース12.2(25)SV2、12.2(27)SV5、および12.2(29)SV3だけです。	Vulnerable.脆弱性が存在するのは、リリース12.2(25)SV2、12.2(27)SV5、および12.2(29)SV3だけです。
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	脆弱性あり。最初の修正はリリース12.4SW	脆弱性あり。最初の修正はリリース15.0M* 12.2(23)SW1までのリリースには脆弱性はありません。
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。
12.2SXI	12.2(33)SXI11	12.2(33)SXI11
12.2日本語	12.2(33)SXJ5	12.2(33)SXJ5
12.2SY	12.2(50)SY4	12.2(50)SY4
12.2SZ	脆弱性なし	脆弱性なし
12.2T	脆弱性なし	脆弱性なし
12.2TPC	脆弱性なし	脆弱性なし
12.2WO	脆弱性なし	脆弱性なし
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	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。最初の修正はリリース12.2SG	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。最初の修正はリリース12.2SG
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
12.2YK	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	脆弱性なし
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	脆弱性なし
12.2ZD	脆弱性なし	脆弱性なし
12.2ZE	脆弱性なし	脆弱性なし
12.2ZH	脆弱性なし	脆弱性なし
12.2ZJ	脆弱性なし	脆弱性なし
12.2ZP	脆弱性なし	脆弱性なし
12.2ZU	脆弱性なし	脆弱性なし
12.2ZX	脆弱性なし	脆弱性なし
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）	2013年3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
12.3	脆弱性なし	脆弱性なし
12.3B	脆弱性なし	脆弱性なし
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15.0M*
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(2)T9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15.0M* 12.3(2)T9までのリリースには脆弱性はありません。

12.3TPC	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。
12.3XA	脆弱性なし	脆弱性なし
12.3XB	脆弱性なし	脆弱性なし
12.3XC	脆弱性なし	脆弱性なし
12.3XD	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M*
12.3XE	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M*
12.3XF	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。
12.3XG	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M*
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12.4T	脆弱性あり。最初の修正はリリース15.0M*
12.3XK	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M*
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15.0M*
12.3XQ	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M*
12.3XR	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M*
12.3XU	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15.0M*
12.3XW	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15.0M*
12.3XX	脆弱性あり。最初の修正はリリース12.4	脆弱性あり。最初の修正はリリース15.0M*
12.3XY	脆弱性なし	脆弱性なし
12.3XZ	脆弱性なし	脆弱性なし
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15.0M*

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 15.0M*
12.3YG	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 15.0M*
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 15.0M*
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 15.0M*
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 15.0M*
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 15.0M*
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 15.0M*
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 15.0M*
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 15.0M*
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 15.0M*
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 15.0M*
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 15.0M*
Affected 12.4-Based Releases	First Fixed Release（修正された最初のリリース）	2013年3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	12.4(25g)	脆弱性あり。最初の修正はリリース 15.0M*
12.4GC	12.4(24)GC5	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

12.4ジャム	12.4(25e)JAMより前のリリースには脆弱性があり、12.4(25e)JAM以降のリリースには脆弱性はありません。12.4JANの任意のリリースに移行 12.4(25e)ジャム	12.4(25e)JAMより前のリリースには脆弱性があり、12.4(25e)JAM以降のリリースには脆弱性はありません。 12.4JAN12.4(25e)JAMの任意のリリースに移行
12.4JAX	脆弱性なし	脆弱性なし
12.4JAZ	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	脆弱性あり。最初の修正はリリース12.4MDB
12.4MDA	12.4(24)MDA11	脆弱性あり。最初の修正はリリース12.4MDB
12.4MDB	12.4(24)MDB	12.4(24)MDB13
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」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。
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15.0M*
12.4SW	12.4(15)SW8a	脆弱性あり。最初の修正はリリース15.0M*
12.4T	12.4(15)T17 12.4(24)T7	脆弱性あり。最初の修正はリリース15.0M*

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 15.0M*
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 15.0M*
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 15.0M*
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 15.0M*
12.4XE	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 15.0M*
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 15.0M*
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 15.0M*
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 15.0M*
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 15.0M*
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	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 15.0M*
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 15.0M*
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 15.0M*
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 15.0M*
12.4XV	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。
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 15.0M*
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 15.0M*
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 15.0M*
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 15.0M*
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	12.4(24)YE7	12.4(24)YE3e
12.4YG	12.4(24)YG4	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3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
15.0EB	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。
15.0ED	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)M4	15.0(1)M10 *
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。
15.0秒	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

	15.1S ‡ 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。	15.1S 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	脆弱性なし	15.0(2)SE1
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。	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。
15.0SQA	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。
15.0SY	15.0(1)SY4	15.0(1)SY4
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）	2013年3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	15.1(2)EY4	脆弱性あり。最初の修正はリリース 15.2S
15.1GC	15.1(2)GC2 15.1(4)GC	15.1(4)GC1
1,510万	脆弱性なし	15.1(4)M6
15.1MR	15.1(3)MR	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	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	† 脚注を参照 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	†脚注を参照 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。	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。	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。
15.1SNG	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。
15.1SNI	脆弱性あり。15.2SNGの任意のリリースに移行	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。
15.1SVA	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。
15.1サービス	脆弱性なし	脆弱性なし
15.1SY	15.1(1)SY1（2013年5月24日に入手可能）	15.1(1)SY1（2013年5月24日に入手可能）
15.1T	15.1(1)T4 15.1(2)T5 15.1(3)T	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）	2013年3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
15.2GC	脆弱性なし	脆弱性あり。15.4Tの任意のリリースに移行
15.2GCA	脆弱性なし	脆弱性あり。15.4Tの任意のリリースに移行
15.2JA	脆弱性なし	15.2(2)JA
15.2JAX	脆弱性なし	脆弱性なし
15.2JB	脆弱性なし	脆弱性なし

15.2JN	脆弱性なし	脆弱性なし
1,520万	脆弱性なし	15.2(4)M3
15.2秒	15.2(2)S2 15.2(4)S1 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)S2 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	脆弱性なし	15.2(2)SA
15.2SNG	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。
15.2SNH	15.2(2)SNH1	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	脆弱性なし	脆弱性なし
15.2T	脆弱性なし	15.2(1)T4（2013年5月3日に入手可能） 15.2(2)T3 15.2(3)T3
Affected 15.3-Based Releases	First Fixed Release（修正された最初のリリース）	2013年3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
影響を受ける 15.3 ベースのリリースはありません。		

* Cisco IOSソフトウェアリリース15.0Mは、2013年4月1日にソフトウェアメンテナンスが終了し、追加のリビルドは行われません。詳細については、サポート終了通知を参照してください。Cisco IOSソフトウェアリリース15.1Mへの移行を検討することをお勧めします。

† Cisco 7600シリーズルータの場合、2013年3月のバンドル公開に含まれるすべてのシスコセキュリティアドバイザリに対する最初の修正リリースは、Cisco IOSソフトウェアリリース15.1(3)S5です。Cisco 7200および7300シリーズルータの場合、2013年3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済みリリースは、Cisco IOSソフトウェアリリース15.1(3)S5aであり、2013年4月15日から利用可能になります。

‡ VRF対応NAT機能は、Cisco 7600シリーズルータで稼働するどのCisco IOSソフトウェアリリースでもサポートされていません。この機能は、一部のリリースではCisco Bug ID CSCta48550(登録ユーザ専用)およびCSCud19257(登録ユーザ専用)に記載されているように設定できることに注意してください

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 は該当しません。

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、お客様のケースのトラブルシューティング時に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-nat

改訂履歴

リビジョン 1.3	2013年4月11日	15.0SEトレインの脆弱性ステータスを更新し、VRF対応およびCisco 7600シリーズルータに関する注記を追加。
リビジョン 1.2	2013年3月28日	「ソフトウェアバージョンと修正」セクションの修正済みソフトウェアの表を更新。
リビジョン 1.1	2013年3月27日	Cisco IOSソフトウェアテーブルの12.4Tを更新します。
リビジョン 1.0	2013年3月27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。