Cisco IOS Software Network Address Translation Vulnerabilities

Advisory ID: cisco-sa-20120926-nat

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-nat

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。

Revision 1.0

For Public Release 2012 September 26 16:00 UTC (GMT)

内容

要約

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 パケットの変換に関する 2 つのサービス拒否（DoS）の脆弱性があります。

変換を必要とするパケットが該当デバイスを通過すると、脆弱性が引き起こされます。

シスコはこれらの脆弱性に対応するための無償ソフトウェア アップデートを提供しています。このアドバイザリは、次のリンク先で確認できます。
http://tools.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、そのアドバイザリで詳述された脆弱性を解決する Cisco IOS ソフトウェア リリース、および 2012 年 9 月にバンドル公開したすべての Cisco IOS ソフトウェアの脆弱性を解決する Cisco IOS ソフトウェア リリース

を記載しています。

個々の公開リンクは、次のリンクにある「Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication」内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

脆弱性が存在する製品

Cisco IOS ソフトウェアが稼働しているシスコ デバイスで NAT が設定されている場合に、脆弱性が存在します。脆弱性のうちの一方に該当するには、NAT がセッション開始プロトコル（SIP）をサポートしている必要があります。
デバイスで NAT が設定されているかどうかは、次の 2 つの方法で確認できます。

- 稼働中のデバイスで NAT が有効か確認する
- 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

稼働中のデバイスで NAT が有効か確認する

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ために推奨される方法は、デバイスにログインし、**show ip nat statistics** コマンドを実行することです。NAT が有効な場合は、「**Outside interfaces**」および「**Inside interfaces**」の各セクションに少なくとも 1 つのインターフェイスが表示されます。次の例は、NAT 機能が有効になっているデバイスでの表示例です。

```
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、インターフェイスの一覧が「**Outside interfaces**」および「**Inside interfaces**」に続く行に表示されることもあります。**show** コマンドで **section** フィルタをサポートしているリリースでは、次の例に示すように、**show ip nat statistics | section interfaces** コマンドを使用して NAT が有効かどうかを確認できます。

```
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

別の確認方法もあります。Cisco IOS ソフトウェアの設定において NAT が有効になっていれば、**ip nat inside** または **ip nat outside** コマンドが異なるインターフェイスに存在します。または NAT Virtual Interface の場合は、**ip nat enable** インターフェイス コマンドが存在していれば有効です。**show configuration | include ip nat** コマンドを使用して NAT 設定が存在するかどうかを確認する例を次に示します。

```
Router> show configuration | include ip nat
 ip nat inside
 ip nat outside
Router>

Router> show configuration | include ip nat
 ip nat enable
Router>
```

Cisco IOS ソフトウェア リリースを確認する

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 **show version** コマンドを実行してシステム バナーを表示させます。「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、続いてバージョンと 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** コマンドがない場合や、表示が異なる場合があります。

次の例は、シスコ製品で Cisco IOS ソフトウェア リリース 15.0(1)M1 が稼働し、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。

```
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_teamRouter> 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
```

Cisco IOS ソフトウェアのリリース命名規則の追加情報は以下のリンクにある「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

脆弱性が存在しない製品

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 への NAT における DoS 脆弱性

NAT SIP Application Layer Gateway (ALG) 機能では、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によって、VoIP ソリューション間に SIP に基づいた Cisco IOS NAT を導入することができます。
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 機能を有効にした場合に発生します。

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 のパケットに対して実行されます。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 コマンドで設定できます。

この脆弱性は、Cisco Bug ID CSCtn76183（ 登録ユーザのみ ）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、ネットワーク間で転送されるパケットの IP アドレスを、必要な場合に変換する機能です。
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。この脆弱性の不正利用に成功した場合、DoS 状態が引き起こされます。

この脆弱性は、Cisco Bug ID CSCtr46123（ 登録ユーザのみ ）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。

脆弱性スコア詳細

シスコはこのアドバイザリでの脆弱性に対して Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。このセキュリティ アドバイザリでの CVSS スコアは CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する組織の手助けとなる標準ベースの評価法です。

シスコは基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供しています。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、自身のネットワークにおける脆弱性の影響度を導き出すことができます。

シスコは次のリンクで CVSS に関する追加情報を提供しています。

http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

また、シスコは個々のネットワークにおける環境影響度を算出する CVSS 計算ツールを次のリンクで提供しています。

http://tools.cisco.com/security/center/cvssCalculator.x/

CSCtn76183 Cisco IOS Software NAT for SIP Denial of Service Vulnerability

Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCtr46123 Cisco IOS Software NAT Denial of Service Vulnerability Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

このアドバイザリに記載された脆弱性の不正利用に成功した場合、該当するデバイスでは再起動が発生することがあります。この脆弱性が繰り返し悪用されると、継続的な DoS 状態となる可能性があります。

ソフトウェア バージョンおよび修正

Cisco IOS ソフトウェア Cisco IOS ソフトウェア テーブル（下記）の各行は Cisco IOS ソフトウェア トレインを示します。あるトレインが脆弱性を含む場合、修正を含む最初のリリースは「First Fixed Release」列に示されます。「First Fixed Release for All Advisories in the September 2012 Bundled Publication」列は、その Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドル公開で公開済みであるすべての脆弱性を修正する最初のリリースを示します。シスコは利用可能な最新のリリースへのアップグレードを推奨します。Cisco IOS ソフトウェア チェッカーを利用して特定の Cisco IOS ソフトウェア リリースに対応したシスコのセキュリティ アドバイザリを検索することができます。このツールは次の Cisco Security Intelligence Operations（SIO）ポータルで利用できます。
http://tools.cisco.com/security/center/selectIOSVersion.x

Major	Availability of Repaired Releases

Release		
Affected 12.0-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the September 2012 Cisco IOS Software Security Advisory Bundled Publication
There are no affected 12.0-based releases		
Affected 12.2-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the September 2012 Cisco IOS Software Security Advisory Bundled Publication
12.2	Not vulnerable	Not vulnerable
12.2B	Not vulnerable	Vulnerable; First fixed in Release 12.4 Releases up to and including 12.2(4)B8 are not vulnerable.
12.2BC	Not vulnerable	Not vulnerable
12.2BW	Not vulnerable	Not vulnerable
12.2BX	Not vulnerable	12.2(15)BX Releases up to and including 12.2(2)BX1 are not vulnerable.
12.2BY	Not vulnerable	Not vulnerable
12.2BZ	Not vulnerable	Not vulnerable
12.2CX	Not vulnerable	Not vulnerable
12.2CY	Not vulnerable	Not vulnerable
12.2CZ	Not vulnerable	Vulnerable; migrate to any release in 12.2S
12.2DA	Not vulnerable	Not vulnerable
12.2DD	Not vulnerable	Not vulnerable
12.2DX	Not vulnerable	Not vulnerable
12.2EU	Not vulnerable	Not vulnerable
12.2EW	Not vulnerable	Not vulnerable
12.2EWA	Not vulnerable	Not vulnerable
12.2EX	Not vulnerable	Vulnerable; First fixed in Release 15.0SE Releases up to and including 12.2(37)EX are not vulnerable.
12.2EY	Not vulnerable	Vulnerable; First fixed in Release 15.1EY Releases up to and including 12.2(46)EY are not vulnerable.
12.2EZ	Not vulnerable	Not vulnerable
12.2FX	Not vulnerable	Not vulnerable
12.2FY	Not vulnerable	Not vulnerable
12.2FZ	Not vulnerable	Not vulnerable
12.2IRA	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRB	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRC	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRD	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRE	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRF	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2IRG	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2IRH	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2IRI	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2IXA	Not vulnerable	Not vulnerable

12.2IXB	Not vulnerable	Not vulnerable
12.2IXC	Not vulnerable	Not vulnerable
12.2IXD	Not vulnerable	Not vulnerable
12.2IXE	Not vulnerable	Not vulnerable
12.2IXF	Not vulnerable	Not vulnerable
12.2IXG	Not vulnerable	Not vulnerable
12.2IXH	Not vulnerable	Not vulnerable
12.2JA	Not vulnerable	Not vulnerable
12.2JK	Not vulnerable	Not vulnerable
12.2MB	Not vulnerable	Not vulnerable
12.2MC	Not vulnerable	Releases up to and including 12.2(15)MC1 are not vulnerable.Releases 12.2(15)MC2b and later are not vulnerable.First fixed in Release 12.4
12.2MRA	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2MRB	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2S	Not vulnerable	Not vulnerable
12.2SB	Not vulnerable	12.2(33)SB13
12.2SBC	Not vulnerable	Vulnerable; First fixed in Release 12.2SB
12.2SCA	Not vulnerable	Vulnerable; First fixed in Release 12.2SCF
12.2SCB	Not vulnerable	Vulnerable; First fixed in Release 12.2SCF
12.2SCC	Not vulnerable	Vulnerable; First fixed in Release 12.2SCF
12.2SCD	Not vulnerable	Vulnerable; First fixed in Release 12.2SCF
12.2SCE	Not vulnerable	Vulnerable; First fixed in Release 12.2SCF
12.2SCF	Not vulnerable	12.2(33)SCF4
12.2SCG	Not vulnerable	Not vulnerable
12.2SE	Not vulnerable	12.2(46)SE1 12.2(55)SE6
12.2SEA	Not vulnerable	Not vulnerable
12.2SEB	Not vulnerable	Not vulnerable
12.2SEC	Not vulnerable	Not vulnerable
12.2SED	Not vulnerable	Not vulnerable
12.2SEE	Not vulnerable	Not vulnerable
12.2SEF	Not vulnerable	Not vulnerable
12.2SEG	Not vulnerable	Not vulnerable
12.2SG	Not vulnerable	12.2(53)SG8 Vulnerable; releases up to and including 12.2(46)SG1 are not vulnerable.
12.2SGA	Not vulnerable	Not vulnerable
12.2SM	Not vulnerable	Not vulnerable
12.2SO	Not vulnerable	Not vulnerable
12.2SQ	Not vulnerable	Releases up to and including 12.2(44)SQ2 are not vulnerable.
12.2SRA	Not vulnerable	Not vulnerable
12.2SRB	Not vulnerable	Not vulnerable
12.2SRC	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2SRD	Not vulnerable	Vulnerable; First fixed in Release 12.2SRE
12.2SRE	Not vulnerable	12.2(33)SRE7
12.2STE	Not vulnerable	Not vulnerable
12.2SU	Not vulnerable	Not vulnerable
12.2SV	Not vulnerable	Not vulnerable

12.2SVA	Not vulnerable	Not vulnerable
12.2SVC	Not vulnerable	Not vulnerable
12.2SVD	Not vulnerable	Not vulnerable
12.2SVE	Not vulnerable	Not vulnerable
12.2SW	Not vulnerable	Not vulnerable
12.2SX	Not vulnerable	Not vulnerable
12.2SXA	Not vulnerable	Not vulnerable
12.2SXB	Not vulnerable	Not vulnerable
12.2SXD	Not vulnerable	Not vulnerable
12.2SXE	Not vulnerable	Not vulnerable
12.2SXF	Not vulnerable	Not vulnerable
12.2SXH	Vulnerable; releases up to and including 12.2(33)SXH7 are not vulnerable.	Vulnerable; releases up to and including 12.2(33)SXH7 are not vulnerable.
12.2SXI	12.2(33)SXI7 Not vulnerable up to 12.2(33)SXI4b	12.2(33)SXI10
12.2SXJ	12.2(33)SXJ1	12.2(33)SXJ4
12.2SY	12.2(50)SY3 Vulnerable Only From 12.2(50)SY through 12.2(50)SY2	12.2(50)SY3
12.2SZ	Not vulnerable	Not vulnerable
12.2T	Not vulnerable	Vulnerable; First fixed in Release 12.4 Releases up to and including 12.2(8)T10 are not vulnerable.
12.2TPC	Not vulnerable	Not vulnerable
12.2WO	Not vulnerable	Vulnerable; First fixed in Release 15.0SG
12.2XA	Not vulnerable	Not vulnerable
12.2XB	Not vulnerable	Not vulnerable
12.2XC	Not vulnerable	Not vulnerable
12.2XD	Not vulnerable	Not vulnerable
12.2XE	Not vulnerable	Not vulnerable
12.2XF	Not vulnerable	Not vulnerable
12.2XG	Not vulnerable	Not vulnerable
12.2XH	Not vulnerable	Not vulnerable
12.2XI	Not vulnerable	Not vulnerable
12.2XJ	Not vulnerable	Not vulnerable
12.2XK	Not vulnerable	Not vulnerable
12.2XL	Not vulnerable	Not vulnerable
12.2XM	Not vulnerable	Not vulnerable
12.2XNA	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2XNB	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2XNC	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2XND	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2XNE	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2XNF	Please see Cisco IOS-XE Software Availability	Please see Cisco IOS-XE Software Availability
12.2XO	Not vulnerable	Vulnerable; First fixed in Release 12.2SG Releases up to and including 12.2(40)XO are not vulnerable.
12.2XQ	Not vulnerable	Not vulnerable

12.2XR	Not vulnerable	Not vulnerable
12.2XS	Not vulnerable	Not vulnerable
12.2XT	Not vulnerable	Not vulnerable
12.2XU	Not vulnerable	Not vulnerable
12.2XV	Not vulnerable	Not vulnerable
12.2XW	Not vulnerable	Not vulnerable
12.2YA	Not vulnerable	Not vulnerable
12.2YC	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YD	Not vulnerable	Not vulnerable
12.2YE	Not vulnerable	Not vulnerable
12.2YK	Not vulnerable	Not vulnerable
12.2YO	Not vulnerable	Not vulnerable
12.2YP	Not vulnerable	Not vulnerable
12.2YT	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2YW	Not vulnerable	Not vulnerable
12.2YX	Not vulnerable	Not vulnerable
12.2YY	Not vulnerable	Not vulnerable
12.2YZ	Not vulnerable	Not vulnerable
12.2ZA	Not vulnerable	Not vulnerable
12.2ZB	Not vulnerable	Not vulnerable
12.2ZC	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2ZD	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2ZE	Not vulnerable	Vulnerable; First fixed in Release 12.4
12.2ZH	Not vulnerable	Vulnerable; First fixed in Release 12.4
12.2ZJ	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2ZP	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.2ZU	Not vulnerable	Not vulnerable
12.2ZX	Not vulnerable	Vulnerable; First fixed in Release 12.2SB
12.2ZY	Not vulnerable	Not vulnerable
12.2ZYA	Not vulnerable	Not vulnerable
Affected 12.3-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2012 Cisco IOS Software Security Advisory Bundled Publication**
There are no affected 12.3-based releases		
Affected 12.4-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2012 Cisco IOS Software Security Advisory Bundled Publication**
12.4	12.4(25g) Vulnerable Only From 12.4(23a) thru 12.4(25f)	12.4(25g)
12.4GC	Releases up to and including 12.4(22)GC1	Vulnerable; contact your support organization

	are not vulnerable.	per the instructions in the Obtaining Fixed Software section of this advisory.
12.4JA	Not vulnerable	Not vulnerable
12.4JAL	Not vulnerable	Not vulnerable
12.4JAX	Not vulnerable	Not vulnerable
12.4JAY	Not vulnerable	Not vulnerable
12.4JDA	Not vulnerable	Not vulnerable
12.4JDC	Not vulnerable	Not vulnerable
12.4JDD	Not vulnerable	Not vulnerable
12.4JDE	Not vulnerable	Not vulnerable
12.4JHA	Not vulnerable	Not vulnerable
12.4JHB	Not vulnerable	Not vulnerable
12.4JHC	Not vulnerable	Not vulnerable
12.4JK	Not vulnerable	Not vulnerable
12.4JL	Not vulnerable	Not vulnerable
12.4JX	Not vulnerable	Not vulnerable
12.4JY	Not vulnerable	Not vulnerable
12.4JZ	Not vulnerable	Not vulnerable
12.4MD	12.4(24)MD7	12.4(24)MD7
12.4MDA	Vulnerable; only releases 12.4(24)MDA1 through 12.4(24)MDA10 are vulnerable.	Vulnerable; releases up to and including 12.4(22)MDA6 are not vulnerable.
12.4MDB	12.4(24)MDB10	12.4(24)MDB10
12.4MR	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.4MRA	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.4MRB	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4SW	Not vulnerable	Not vulnerable
12.4T	Vulnerable; only releases 12.4(15)T13 through 12.4(24)T6 are vulnerable.	12.4(24)T8
12.4XA	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XB	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XC	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XD	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XE	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XF	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XG	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XJ	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XK	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XL	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.4XM	Not vulnerable	Releases up to and including 12.4(15)XM are not vulnerable.Releases 12.4(15)XM3 and later are not vulnerable.First fixed in Release 12.4T
12.4XN	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.4XP	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.

12.4XQ	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XR	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XT	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XV	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.4XW	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XY	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XZ	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4YA	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4YB	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.4YD	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
12.4YE	Vulnerable; First fixed in Release 12.4T Releases up to and including 12.4(22)YE6 are not vulnerable.	Vulnerable; First fixed in Release 12.4T
12.4YG	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
Affected 15.0-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2012 Cisco IOS Software Security Advisory Bundled Publication**
15.0EX	Not vulnerable	Not vulnerable
15.0EY	Not vulnerable	Not vulnerable
15.0M	15.0(1)M8	15.0(1)M9
15.0MR	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
15.0MRA	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
15.0S	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.0(1)S6 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0SE	Not vulnerable	15.0(2)SE
15.0SG	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.0(2)SG5 15.0(2)SG6; Available on 11-OCT-12 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0SY	Not vulnerable	15.0(1)SY2
15.0XA	Vulnerable; First fixed in Release 15.1T	Vulnerable; First fixed in Release 15.1M
15.0XO	Cisco IOS XE devices: Please see Cisco IOS-XE Software Availability	Cisco IOS XE devices: Please see Cisco IOS-XE Software Availability
Affected 15.1-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2012 Cisco IOS Software Security Advisory Bundled Publication**

15.1EY	Not vulnerable	15.1(2)EY4
15.1GC	15.1(2)GC2	Vulnerable; First fixed in Release 15.1M
15.1M	15.1(4)M3	15.1(4)M5
15.1MR	Not vulnerable	15.1(3)MR; Available on 01-OCT-12
15.1S	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	 15.1(3)S Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.1SG	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.1(1)SG1 15.1(2)SG 12-NOV-12 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.1SNG	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
15.1SNH	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
15.1SNI	Not vulnerable	Vulnerable; migrate to any release in 15.2SNG
15.1SV	Not vulnerable	Vulnerable; contact your support organization per the instructions in the Obtaining Fixed Software section of this advisory.
15.1T	15.1(2)T5 15.1(3)T3	Vulnerable; First fixed in Release 15.1M
15.1XB	Vulnerable; First fixed in Release 15.1T	Vulnerable; First fixed in Release 15.1M
Affected 15.2-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the September 2012 Cisco IOS Software Security Advisory Bundled Publication**
15.2GC	15.2(2)GC	Releases prior to 15.2(3)GC are vulnerable; Releases 15.2(3)GC and later are not vulnerable.First fixed in Release 15.2T
15.2JA	Not vulnerable	Not Vulnerable
15.2M	Not vulnerable	 Not vulnerable
15.2S	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.2(1)S2 15.2(2)S1 15.2(4)S Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.2SNG	Not vulnerable	Not vulnerable
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; Available on 12-OCT-12

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は受けません。

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は受けません。

回避策

Cisco IOS ソフトウェアの SIP への 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、UDP での NAT SIP ALG 変換を無効にすることで回避することができます。このコマンドは、NAT ALG SIP 機能を含んでいる Cisco IOS イメージでのみ設定できます。レイヤ 3 NAT 変換は引き続き SIP パケットに対して実行できますが、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の入手

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。ソフトウェアの導入を行う前に、お客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境に特有の問題に関してご確認ください。

お客様がインストールしたりサポートを受けたりできるのは、ご購入いただいたフィーチャ セットに対してのみとなります。そのようなソフトウェア アップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載のシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、Cisco.com の Software Navigator からアップグレードを入手することができます。http://www.cisco.com/cisco/software/navigator.html

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、適切な処置について支援を受けてください。

回避策の効果は、使用製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などのお客様の状況に依存します。影響製品およびリリースが多種多様であるため、回避策を実際に展開する前に、対象とするネットワークで適用する回避策または修正が最適であるか、お客様のサービス プロバイダーやサポート会社にご相談ください。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティ ベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、

Cisco Technical Assistance Center（TAC）に連絡してアップグレードを入手してください。

- +1 800 553 2447（北米内からのフリー ダイヤル）
- +1 408 526 7209（北米以外からの有料通話）
- 電子メール：tac@cisco.com

無償アップグレードの対象であることをご証明いただくために、製品のシリアル番号と、このアドバイザリの URL をご用意ください。サービス契約をご利用でないお客様は TAC を通して無償アップグレードをお求めください。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、シスコ ワールドワイドお問い合わせ先を参照してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

不正利用事例と公式発表

Cisco Product Security Incident Response Team（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とその公表は確認しておりません。

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時に発見されました。

この通知のステータス：FINAL

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を示唆するものでもありません。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。またシスコシステムズはいつでも本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

このアドバイザリは次のリンクにある Cisco Security Intelligence Operations に掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-nat

また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の電子メールで配信されています。

- cust-security-announce@cisco.com
- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net

- full-disclosure@lists.grok.org.uk

このアドバイザリに関する今後の更新があれば、Cisco.com に掲載されますが、メーリング リストで配信されるとは限りません。このアドバイザリの URL で更新をご確認いただくことができます。

更新履歴

Revision 1.0	2012-September-26	Initial public release.

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関する支援、およびシスコからセキュリティ情報を入手するための登録方法について詳しく知るには、Cisco.com の http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html にアクセスしてください。この Web ページには、シスコのセキュリティ アドバイザリに関してメディアが問い合わせる際の指示が掲載されています。すべてのシスコ セキュリティ アドバイザリは、http://www.cisco.com/go/psirt/ で確認することができます。