Cisco Security Advisory: Cisco IOS Software Network Address Translation Vulnerability

Advisory ID: cisco-sa-20120328-nat

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-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 March 28 16:00 UTC (GMT)

目次

要約

Cisco IOS ソフトウェアの Network Address Translation（NAT）機能には、Session Initiation Protocol（SIP）パケットの変換に関する Denial of Service（DoS）の脆弱性が存在します。

該当デバイスをパケットが通過するとき、そのパケットが SIP ペイロード部分の変換を必要とする場合に脆弱性の影響を受けます。

シスコはこの脆弱性に対処する無償のソフトウェア アップデートをリリースしました。この脆弱性に対しては回避策があります。

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-20120328-nat

注：2012 年 3 月 28 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。各アドバイザリには、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 3 月 にバンドル公開したすべて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_mar12.html

該当製品

脆弱性が存在する製品

Cisco IOS ソフトウェアを実行しているシスコ デバイスで、NAT が設定されており、かつ SIP に対する NAT のサポートが含まれる場合、脆弱性が存在します。

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で存在しています。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。

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、この脆弱性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 NAT SIP のメモリ枯渇に関する脆弱性

SIP パケットの NAT SIP Application Level Gateway（ALG）変換は、メモリ リソースの枯渇状態を引き起こす場合があり、これによって該当デバイスの再起動を引き起こし DoS 状態が発生する可能性があります。

SIP に対する NAT は、UDP ポート 5060 パケットで実行するよう初期設定されています。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 CSCti35326（ 登録ユーザのみ ）に文書化されており、Common

Vulnerabilities and Exposures ID として CVE-2012-0383 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

Cisco IOS Software NAT SIP Memory Starvation 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

この脆弱性が不正利用されると、メモリの使用量が増大し、デバイスが再起動されるまで解放されなくなります。このメモリの消費によって、該当するデバイスには DoS 状態が発生し、デバイスが応答しなくなったり、再起動したりす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である場合、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 March 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）ポータルで入手できます。
http://tools.cisco.com/security/center/selectIOSVersion.x

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the March 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 March Cisco IOS Software Security Advisory Bundled Publication
There are no affected 12.2 based releases		
Affected 12.3-Based Releases	First Fixed Release	First Fixed Release for All Advisories in the March 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 March Cisco IOS Software Security Advisory Bundled Publication
12.4	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4GC	Releases up to and including 12.4(24)GC3a are not vulnerable.	Vulnerable; contact your support organization per instructions in Obtaining Fixed Software section o advisory.
12.4JA	Not vulnerable	12.4(23c)JA4 12.4(25e)JA
12.4JAX	Not vulnerable	Vulnerable; First fixed in Release 12.4JA
12.4JDA	Not vulnerable	Vulnerable; contact your support organization per instructions in Obtaining Fixed Software section o advisory.
12.4JDC	Not vulnerable	Vulnerable; contact your support organization per instructions in Obtaining Fixed Software section o advisory.
12.4JDD	Not vulnerable	Vulnerable; contact your support organization per instructions in Obtaining Fixed Software section o advisory.
12.4JDE	Not vulnerable	Vulnerable; contact your support organization per instructions in Obtaining Fixed Software section o advisory.
12.4JHA	Not vulnerable	Vulnerable; contact your support organization per instructions in Obtaining Fixed Software section o advisory.
12.4JHB	Not vulnerable	Vulnerable; contact your support organization per

		instructions in Obtaining Fixed Software section o advisory.
12.4JHC	Not vulnerable	Vulnerable; contact your support organization per instructions in Obtaining Fixed Software section o advisory.
12.4JK	Not vulnerable	Vulnerable; contact your support organization per instructions in Obtaining Fixed Software section o advisory.
12.4JL	Not vulnerable	Vulnerable; contact your support organization per instructions in Obtaining Fixed Software section o advisory.
12.4JX	Not vulnerable	Vulnerable; First fixed in Release 12.4JA
12.4JY	Not vulnerable	Vulnerable; First fixed in Release 12.4JA
12.4JZ	Not vulnerable	Vulnerable; First fixed in Release 12.4JA
12.4MD	Only releases 12.4(24)MD5 and 12.4(24)MD6 are vulnerable.	12.4(22)MD3; Available on 30-MAR-12
12.4MDA	Releases 12.4(24)MDA5 and prior are not vulnerable; first fixed in 12.2(24)MDA11	12.4(24)MDA11
12.4MDB	12.4(24)MDB4	12.4(24)MDB5a
12.4MDC	Not vulnerable	Not vulnerable
12.4MR	Not vulnerable	Vulnerable; contact your support organization per instructions in Obtaining Fixed Software section o advisory.
12.4MRA	Not vulnerable	Vulnerable; contact your support organization per instructions in Obtaining Fixed Software section o advisory.
12.4MRB	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4SW	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4T	Only releases 12.4(24)T5 and 12.4(24)T6 are vulnerable.	12.4(15)T17 12.4(24)T7
12.4XA	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4XB	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XC	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4XD	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4XE	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4XF	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4XG	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4XJ	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4XK	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4XL	Not vulnerable	Vulnerable; contact your support organization per instructions in Obtaining Fixed Software section o advisory.
12.4XM	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4XN	Not vulnerable	Vulnerable; contact your support organization per instructions in Obtaining Fixed Software section o advisory.
12.4XP	Not vulnerable	Vulnerable; contact your support organization per instructions in Obtaining Fixed Software section o advisory.
12.4XQ	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4XR	Not vulnerable	Vulnerable; First fixed in Release 12.4T
12.4XT	Not vulnerable	Vulnerable; First fixed in Release 15.0M

12.4XV	Not vulnerable	Vulnerable; contact your support organization per instructions in Obtaining Fixed Software section o advisory.
12.4XW	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4XY	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4XZ	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4YA	Not vulnerable	Vulnerable; First fixed in Release 15.0M
12.4YB	Not vulnerable	Vulnerable; contact your support organization per instructions in Obtaining Fixed Software section o advisory.
12.4YD	Not vulnerable	Vulnerable; contact your support organization per instructions in Obtaining Fixed Software section o advisory.
12.4YE	Not vulnerable	12.4(24)YE3d
12.4YG	Not vulnerable	12.4(24)YG4
Affected 15.0-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the March Cisco IOS Software Security Advisory Bundled Publication**
15.0M	Only releases 15.0(1)M4 and 15.0(1)M5 are vulnerable.	15.0(1)M8
15.0MR	Not vulnerable	Vulnerable; contact your support organization per instructions in Obtaining Fixed Software section o advisory.
15.0MRA	Not vulnerable	Vulnerable; contact your support organization per instructions in Obtaining Fixed Software section o advisory.
15.0S	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.0(1)S5 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0SA	Not vulnerable	Not vulnerable
15.0SE	Not vulnerable	15.0(1)SE1
15.0SG	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.0(2)SG2 Cisco IOS XE devices: Please see Cisco IOS XE Software Availability
15.0SY	Not vulnerable	15.0(1)SY1
15.0XA	Not vulnerable	Vulnerable; First fixed in Release 15.1T
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 March Cisco IOS Software Security Advisory Bundled Publication**
15.1EY	Not vulnerable	15.1(2)EY2
15.1GC	Not vulnerable	15.1(2)GC2
15.1M	Not vulnerable	15.1(4)M4; Available on 30-MAR-12
15.1MR	Not vulnerable	Vulnerable; contact your support organization per instructions in Obtaining Fixed Software section o advisory.
15.1S	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability	15.1(3)S2 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	Not vulnerable Cisco IOS XE devices: Please see Cisco IOS XE Software Availability

15.1SNG	Not vulnerable	Vulnerable; contact your support organization per instructions in Obtaining Fixed Software section o advisory.
15.1SNH	Not vulnerable	Not vulnerable
15.1T	15.1(1)T4 15.1(2)T5; Available on 27-APR-12 15.1(3)T	15.1(3)T3
15.1XB	Not vulnerable	Vulnerable; First fixed in Release 15.1T
Affected 15.2-Based Releases	**First Fixed Release**	**First Fixed Release for All Advisories in the March Cisco IOS Software Security Advisory Bundled Publication**
There are no affected 15.2 based releases		

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、2012 年 3 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。

回避策

SIP に対する NAT におけるリソース枯渇に関する脆弱性

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。

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。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 または http://www.cisco.com/public/sw-center/sw-usingswc.shtml 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。

ソフトウェアのアップグレードに関し、psirt@cisco.com もしくは security-alert@cisco.com にお問い合わせいただくことはご遠慮ください。

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 Center 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

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 へのサービス リクエストの対応の際に発見されました。

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-20120328-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-March-28	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。