Cisco IOS ソフトウェアのネットワーク アドレス変換における Denial of Service（DoS）の脆弱性

High

アドバイザリーID : cisco-sa-20140924-nat

初公開日 : 2014-09-24 16:00

バージョン 1.0 : Final

CVSSスコア : 7.1

回避策 : No Workarounds available

Cisco バグ ID : CSCun54071

CVE-2014-3361

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）機能の脆弱性はリモート攻撃者非認証により影響を受けたデバイスのサービス拒否（DoS）条件を引き起こすようにする可能性があります。 脆弱性は IPバージョンの不適当な変換が原因 4 つの（IPv4）パケットです。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。

このアドバイザリは、次のリンクより確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140924-nat

注: 2014 年 9月 24 日、Cisco IOSソフトウェア Security Advisory によって組み込まれる書は 6 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ます。 個々の公表資料へのリンクは、次のリンクにある「*シスコのイベント対応：半年ごと Cisco IOSソフトウェア Security Advisory は次のリンクでパブリケーションを組み込みました*:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep14.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 リリースを実行している Ciscoデバイスはセッション開始プロトコル（SIP）のマルチパート Session Description Protocol （SDP）のための NAT および NAT アプリケーション層ゲートウェイ（NAT ALG）で設定されたとき脆弱 有効に なりました です。 SIP のマルチパート SDP のための NAT ALG はデフォルトで有効に なりません。

Cisco IOSデバイスが NAT のために設定されるかどうか判別する 2 つのメソッドがあります:

- NAT がデバイスでアクティブであるかどうか判別して下さい
- Nat コマンドがデバイスコンフィギュレーションに含まれているかどうか判別して下さい

NAT が Cisco IOSデバイスで有効に なるかどうか確かめる好まれる方法は NAT がデバイスでアクティブであるかどうか判別することです。

1 つのメソッドは SIP のマルチパート SDP のための NAT ALG が有効に なるかどうか判別して利用できます。

NAT がデバイスでアクティブであるかどうか判別して下さい

NAT がデバイスに Cisco IOSソフトウェアを、ログイン実行する Ciscoデバイスでアクティブ判別しである、 **show ip nat statistics コマンドを**発行するためかどうか。 NAT がアクティブである場合、「Outside インターフェイス」および「内部インターフェイス」セクション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ています。 NAT がアクティブどこにであるか次の例にデバイスに示されています:

```
Router#show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Peak translations: 10, occurred 00:24:01 ago
Outside interfaces:
  FastEthernet0/0
Inside interfaces:
  FastEthernet0/1
Hits: 134280  Misses: 0
CEF Translated packets: 134270, CEF Punted packets: 10
Expired translations: 11
Dynamic mappings:
-- Inside Source
[Id: 1] access-list NET-192.168.20.0_24 pool POOL-NET-192.168.1.0_24 refcount 0
 pool POOL-NET-192.168.1.0_24: netmask 255.255.255.0
start 192.168.1.120 end 192.168.1.128
type generic, total addresses 9, allocated 0 (0%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
Router#
```

インターフェイスが **show ip nat statistics コマンド**の出力にリストされていない場合、NAT はまだ NAT 仮想インターフェイス 機能を通してデバイスでアクティブかもしれません。 NAT がこの機能を通してアクティブであるかどうか判別するために、 **提示 IP NAT nvi statistics コマンドを**発行して下さい。 NAT がアクティブである場合、「NAT 使用可能なインターフェイス」セクションは少なくとも 1 つのインターフェイスが含まれています。 NAT がアクティブ

どこにであるか次の例にデバイスに示されています:

```
Router#show ip nat nvi statistics
Total active translations: 1 (0 static, 1 dynamic; 1 extended)
NAT Enabled interfaces:
  FastEthernet0/0, FastEthernet0/1
Hits: 81373  Misses: 3
CEF Translated packets: 44371, CEF Punted packets: 8
Expired translations: 3
Dynamic mappings:
-- Source [Id: 1] access-list NET-192.168.20.0_24 pool POOL-NET-192.168.1.0_24 refcount 1
 pool POOL-NET-192.168.1.0_24: netmask 255.255.255.0
start 192.168.1.120 end 192.168.1.128
type generic, total addresses 9, allocated 1 (11%), misses 0
Router#
```

Nat コマンドがデバイスコンフィギュレーションにあるかどうか判別して下さい

NAT が Cisco IOSソフトウェア 設定で、デバイスへのログイン判別し有効に なった、 **show running-config コマンドを**発行するためかどうか。 NAT がアクティブである場合、 **ip nat inside** および **ip nat outside interface コマンドは**ある必要があります。 また、 NAT 仮想インターフェイスの場合には、 **IP NAT イネーブル** interface コマンドはあります。

注: デバイスの Cisco Easy VPN Remote クライアント機能 設定は自動的に NAT を有効に します。 NAT および Cisco Easy VPN Remote 機能によって作成されるポート アドレス変換（PAT）コンフィギュレーションは始動か実行コンフィギュレーション ファイルに書き込まれません。 しかしこれらのコンフィギュレーションは **show ip nat statistics コマンド**を使用して表示することができます。

SIP のマルチパート SDP のための NAT ALG がデバイスコンフィギュレーションで有効に なるかどうか判別して下さい

Cisco IOSソフトウェアを実行する Cisco IOSデバイスで有効に なるべき SIP トラフィックのマルチパート SDP の NAT ALG に関しては **IP NAT サービス許可マルチパート** コマンドはデバイスコンフィギュレーションにある必要があります。 次の例は NAT が SIP のマルチパート SDP のための ALG 有効に なる デバイスを示したものです:

```
Router#show running-config | include ip nat service allow-multipart
ip nat service allow-multipart
Router#
```

デバイスの Cisco IOS ソフトウェア リリースを判別して下さい

シスコ製品上で動作している Cisco IOS ソフトウェア リリースについては、管理者がデバイスにログインして **show version** コマンドを発行し、システム バナーを表示することで判別できます。 "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、Cisco IOS ソフトウェア リリースが 15.2(4)M5、インストールされたイメージ名が C3900-UNIVERSALK9-M であるシスコ製品を示しています。

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), 15.2(4)M5, RELEASE SOFTWARE
(fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Fri 13-Sep-13 16:44 by prod_rel_team
```

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), 15.2(4)M5, RELEASE SOFTWARE
(fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Fri 13-Sep-13 16:44 by prod_rel_team
```

Cisco IOS ソフトウェア リリースの命名規則については、以下を参照してください。[ホワイトペーパー： Cisco IOS および NX-OS ソフトウェア リファレンス ガイド]

脆弱性を含んでいないことが確認された製品

ネットワークアドレス交換 機能が Cisco IOSソフトウェアを実行する Ciscoデバイスで設定されない場合デバイスは脆弱ではないです。 ネットワークアドレス交換 機能が Cisco IOSソフトウェアを実行する Ciscoデバイスで設定されるが SIP のマルチパート SDP のための NAT ALG が有効に ならない場合、デバイスは脆弱ではないです。

以下の製品はずっと確認された脆弱です:

- Cisco IOS XR ソフトウェア
- Cisco IOS XE 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ソフトウェアのアプリケーション層ゲートウェイ（ALG）モジュールの脆弱性は非認証により、リモート攻撃者 サービス拒否 （DoS）に状態を導く可能性がある影響を受けたデバイスのリロードを引き起こすようにする可能性があります。

脆弱性はネットワーク アドレス変換（NAT）を必要とするセッション開始プロトコル（SIP） メッセージが影響を受けたデバイスでどのようにが処理されるか原因です。 攻撃者は影響を受けたデバイスによって処理され、変換された巧妙に細工された SIP メッセージの送信によってこの脆弱性を不正利用する可能性があります。 エクスプロイトは攻撃者により影響を受けたデバイスは

リロードしますことを可能にする可能性がありま DoS 状態に導きます。

この脆弱性はマルチパート SDP トラフィックがデバイスで（RFC 5621 で定義されたように）SIP のマルチパート SDP のための NAT および NAT ALG を有効に なる経るとき引き起こすことができます。 SIP のマルチパート SDP のための NAT ALG はデフォルトで有効に なりません。 この脆弱性は影響を受けたデバイスを通過するトラフィックによってだけ引き起こし、デバイス自体に向かうトラフィックと不正利用することができません。 この脆弱性は IP バージョン 6(IPv6) トラフィックと不正利用することができません。

この脆弱性 Cisco バグ ID CSCun54071 （ 登録ユーザのみ ）で文書化されています、よくある脆弱性および公開（CVE）ID CVE-2014-3361 は割り当てられました。

回避策

この脆弱性は SIP のマルチパート SDP のための NAT ALG をディセーブルにすることによって軽減することができます。 SIP のマルチパート SDP のための NAT ALG をディセーブルにするために、許可 **マルチパート** グローバル コンフィギュレーション モードで **no ip nat サービスを**利用して下さい。

注: SIP のマルチパート SDP のための NAT ALG をディセーブルにすることはサード パーティ SIP ゲートウェイおよびデバイスとの相互運用性に悪影響を及ぼすかもしれません。

修正済みソフトウェア

ソフトウェアアップグレードを検討するとき、顧客は Cisco Security Advisory、応答および表記アーカイブを http://www.cisco.com/go/psirt で参照し、公開および完全なアップグレード ソリューションを判別するためにそれに続くアドバイザリを検討するように勧告されます。

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

Cisco は顧客が Cisco IOSソフトウェアの脆弱性への公開を判別するのを助けるようにツールを提供しました。 Cisco IOS Software Checker により、次のタスクを実行できます。

- ドロップダウン メニューからリリースを選択するか、ローカル システムからファイルをアップロードすることによって、検索を開始する
- **show version** コマンドの出力をツールで解析する
- 2015 年 9 月組み込まれた書にすべての以前に公開された Cisco Security Advisory、特定のパブリケーション、またはすべてのアドバイザリを含めることによってカスタマイズされた検索を作成して下さい

ツールは各 Cisco Security Advisory のすべての脆弱性を解決する以前のリリースおよび問い合わせられたソフトウェア リリースに影響を与える Cisco Security Advisory を識別します（「最初に」固定される）。 該当する場合、ツールはまた最も早い可能性のある リリースを戻しますすべての表示する アドバイザリのすべての脆弱性を解決する（「結合される最初に」固定される）。 Cisco IOSソフトウェア チェッカーを単に参照するか、または次のフィールドでこの組み込まれたパブリケーションのアドバイザリの何れかから影響を受けるかどうか判別するために Cisco IOS ソフトウェア リリースを入力して下さい。

（入力例： 15.1(4)M2）

Cisco IOS XE ソフトウェア

Cisco IOS XE ソフトウェアはこの文書で表われる脆弱性から影響を受けません。

Cisco IOS XR ソフトウェア

Cisco IOS XR ソフトウェアは 2014 年 9 月 Cisco IOSソフトウェア Security Advisory によって組み込まれる書で表われる脆弱性の何れかから影響を受けません。

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エクスプロイト事例やその公表を確認していません。

この脆弱性は弊社販売代理店 要求の処理の間に識別されました。

出典

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140924-nat

改訂履歴

リビジョン 1.0	2014-September-24	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。