# 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-20170927-nat

**初公開日 :** 2017-09-27 16:00

**バージョン 1.0 :** Final

**CVSSスコア :** 8.6

**回避策 :** Yes

**Cisco バグ ID :** CSCvc57217

CVE-2017-12231

**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 ソフトウェアには、ネットワーク アドレス変換（NAT）の実装に脆弱性があり、認証されていないリモート攻撃者により、該当するデバイスに Denial of Service（DoS）の状態が引き起こされる可能性があります。

この脆弱性は、RAS（登録、許可、状態）プロトコルを使用する H.323 メッセージの不適切な変換に起因するもので、IPv4 パケットを介して該当するデバイスに送信されます。 攻撃者が、該当するデバイスを介して巧妙に細工された H.323 RAS パケットを送信することにより、この脆弱性を不正利用する可能性があります。 不正利用に成功すると、攻撃者により該当デバイスのクラッシュとリロードが引き起こされ、その結果 DoS 状態が発生する可能性があります。

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。この脆弱性に対処する回避策はありません。

このアドバイザリは、次のリンクより確認できます。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-nat

このアドバイザリは、2017 年 9 月 27 日に公開された 13 件の脆弱性に関する 12 件のシスコ セキュリティ アドバイザリを含む Cisco IOS ソフトウェアおよび IOS XE ソフトウェア リリースのセキュリティ アドバイザリ バンドルの一部です。 これらのアドバイザリとリンクの一覧については、以下を参照してください。シスコのイベント対応： 9月 2017 年半年ごと Cisco IOS および IOS XE ソフトウェア Security Advisory によって組み込まれる書。

## 該当製品

# 脆弱性のある製品

この脆弱性は、次のすべての条件を満たすシスコ製デバイスに影響を及ぼします。

- デバイスが Cisco IOS ソフトウェアの脆弱なリリースを実行している。 Cisco IOS ソフトウェア リリースが脆弱である情報に関しては、このアドバイザリの修正済みソフトウェアのセクションを参照して下さい。
- デバイスが NAT を実行するように構成されている。
- デバイスが H.323 RAS メッセージ用に NAT（NAT ALG）でアプリケーション層ゲートウェイを使うように構成されている。 NAT ALG は、H.323 RAS メッセージに対してデフォルトで有効となっています。

この脆弱性は、NAT 仮想インターフェイス機能、もしくは Cisco IOS ソフトウェアの Cisco Easy VPN リモート クライアント機能を介して NAT を実行するように構成されたデバイスには影響を及ぼしません。

## NAT 設定の検証

デバイスが NAT を実行するように構成されているか調べるには、管理者は NAT がデバイス上でアクティブになっているか（推奨）、または NAT コマンドがデバイス構成に存在するかを確認します。

、管理者はデバイスにログイン NAT がデバイスでアクティブであるかどうか判別し、CLI の **show ip nat statistics コマンドを**発行するためにできます。 NAT がアクティブである場合、コマンド 出力の *Outside インターフェイス*および*内部インターフェイス* セクションは少なくとも 1 つのインターフェイスが含まれています。

次の例は NAT がアクティブであるデバイスのための **show ip nat statistics コマンド**の出力を示したものです:

```
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#
```

**show ip nat statistics コマンド**の出力がインターフェイスをリストしなかったものではなく場合、NAT はデバイスで非アクティブです。

また、管理者は NAT が CLI の **show running-config コマンドを**発行することおよび 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査定ことをによってデバイスでアクティブであるかどうか判別できます。 NAT がデバイスでアクティブである場合、**show running-config コマンド**の出力は **ip nat inside** および **ip nat outside interface コマンドが**含まれています。

## H.323 RAS に対して NAT ALG が有効か確認する

デフォルトでは、H.323 RAS メッセージに対して NAT ALG が有効になっており、NAT ALG はデバイスの実行中の設定情報には表示されません。

H.323 RAS メッセージ、管理者のための NAT ALG のステータスを口グイン判別し、**show running-config を**発行することはデバイスにできます | CLI に **IP NAT サービス RAS** コマンドを、**含めて下さい**たとえば:

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

no ip nat service ras
Router#
```

前述の例では、NAT ALG は **no ip nat サービス RAS** 出力によって示されるように H.323 RAS メッセージのために無効、です。

**show running-config** のための出力がなければ **| IP NAT サービス RAS** コマンドを、NAT ALG 有効に されます H.323 RAS メッセージのために**含んで下さい**。

## Cisco IOS ソフトウェア リリースの判別

デバイス上で実行されている Cisco IOS ソフトウェア リリースは、管理者がデバイスに口グインして、CLI で **show version** コマンドを使用し、表示されるシステム バナーを参照することにより確認できます。 デバイスが Cisco IOS ソフトウェアを実行している場合、システム バナーに「*Cisco Internetwork Operating System Software*」や「*Cisco IOS Software*」などのテキストが表示されます。 バナーにはインストールされたイメージ名もカッコ内に表示されます。その後ろには Cisco IOS ソフトウェアのリリース番号とリリース名も表示されます。 一部のシスコ デバイスでは、**show version** コマンドをサポートしていなかったり、別の出力が表示されたりすることがあります。

次の例は Cisco IOS ソフトウェア リリース 15.5(2)T1 を実行して、*C2951-UNIVERSALK9-M*

のインストール済みイメージ名前があるデバイスのためのコマンドの出力を示したものです:

```
Router> show version

Cisco IOS Software, C2951 Software (C2951-UNIVERSALK9-M), Version 15.5(2)T1, RELEASE SOFTWARE
(fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Mon 22-Jun-15 09:32 by prod_rel_team
.
.
.
```

Cisco IOS ソフトウェア リリースの命名と番号付けの規則については、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

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。

Cisco IOS ソフトウェアを実行しており、NAT 仮想インターフェイス機能、もしくは Cisco Easy VPN リモート クライアント機能を介して NAT を実行するように構成されたデバイスには、この脆弱性の影響が及ばないことを、シスコは確認しました。

また、この脆弱性が Cisco IOS XE ソフトウェア、Cisco IOS XR ソフトウェア、Cisco NX-OS ソフトウェアには影響を与えないことも確認しました。

さらに、この脆弱性は Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスにも影響を及ぼさないことを確認しました。

### 詳細

このアドバイザリで説明する脆弱性は、該当するデバイスで、ソフトウェアが NAT を実行し、H.323 RAS メッセージに対して NAT ALG を使用するように構成されている場合に、RAS ( 登録、許可、状態 ) プロトコルを使用する H.323 メッセージが適切に変換されないことに起因しています。 認証されていないリモートの攻撃者が、該当するデバイスを介して巧妙に細工された H.323 RAS パケットを送信することで、この脆弱性を不正利用し、デバイスのクラッシュとリロードを引き起こして、DoS 状態を発生させる可能性があります。

この脆弱性が不正利用されるのは、該当するデバイスを経由して送信される IPv4 パケットのトラフィックのみです。 該当するデバイスでトラフィックが終了する場合は、不正利用されることはありません。 また、IPv6 トラフィックの場合も、不正利用されることはありません。

### セキュリティ侵害の痕跡

### 回避策

管理者は、H.323 RAS メッセージの NAT ALG を無効にすることで、この脆弱性を緩和できる場合があります。 ただし、該当するデバイスを通じて RAS トラフィックの送受信を行うデバイスでの通常の運用に望ましくない影響が及ぶ可能性があります。その結果、通常のネットワーク運用が阻害される可能性があります。 管理者は、同機能を無効にする前に、ネットワーク環境で NAT ALG の H.323 RAS メッセージが必要ないかどうかを必ず確認してください。 H.323 RAS メッセージのための NAT ALG の使用をディセーブルにするために、管理者はグローバル コンフィギュレーション モードで **no ip nat サービス RAS** コマンドを使用できます。

## 修正済みソフトウェア

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。 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、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ 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、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、お客様は以下のリンクに記載された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。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。 通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。 無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

ソフトウェアのアップグレードを検討する際には、Cisco Security Advisories and Alerts ページで入手できるシスコ製品のアドバイザリを定期的に参照して、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。

### 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 TAC に連絡してアップグレードを入手してください。
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

## Cisco IOS ソフトウェア

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ために Cisco はツールを、各アドバイザリに説明がある脆弱性を解決する以前のリリースおよび特定の Cisco IOS ソフトウェア リリースに影響を与える Cisco Security Advisory を識別する Cisco IOSソフトウェア チェッカー提供します、（「最初に」固定される）。 また該当する場合、すべてのアドバイザリに記載されたすべての脆弱性が修正された最初のリリース（「Combined First Fixed」）を特定できます。

このツールを使用して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（複数可）を選択するか、分析対象となるローカル システムからファイルをアップロードして、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
- カスタマイズした検索（過去に公開されたすべてのシスコ セキュリティ アドバイザリを検索対象に含めたり、特定のアドバイザリのみ、または最新のバンドル資料から全アドバイザリを含めるなど）を作成する

リリースがあらゆる公開された Cisco Security Advisory から影響を受けするかどうか判別するために、Cisco.com の Cisco IOSソフトウェア チェッカーを使用するか、または—次のフィールドで… Cisco IOS ソフトウェア リリースを—たとえば、**15.1(4)M2** 入力して下さい:

## 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。

## 出典

この脆弱性は、Jason Fernandez によってシスコに報告されました。

## URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-nat

## 改訂履歴

| Version | Description | Section | Status | 日付 |
|---|---|---|---|---|
| 1.0 | 初回公開リリース | | Final | 2017 年 9 月 27 日 |

## 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。