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

アドバイザリーID : cisco-sa-20170927-nat CVE-2017-12231
初公開日 : 2017-09-27 16:00
最終更新日 : 2022-12-16 21:17
バージョン 1.1 : Final
CVSSスコア : 8.6
回避策 : Yes
Cisco バグ ID : CSCvc57217

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、登録、アドミッション、ステータス(RAS)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し、IPv4パケットを介して該当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。

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://sec.cloudapps.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。アドバイザリとリンクの一覧については、『Cisco Event Response: September 2017 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication』を参照してください。

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。脆弱性が存在する Cisco IOS ソフトウェア リリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。
- 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。

NAT がデバイス上でアクティブかどうかを確認するには、管理者はデバイスにログインして、CLI で show ip nat statistics コマンドを実行できます。NAT がアクティブの場合は、コマンドの出力で Outside interfaces と Inside interfaces のセクションに、少なくともインターフェイスが 1 つ表示されます。

次の例は、NAT がアクティブなデバイスに対する show ip nat statistics コマンドの出力を示しています。

<#root>

```
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 コマンドの出力にインターフェイスが含まれていない場合、そのデバイスでは NAT はアクティブになっていません。

また、管理者は CLI で show running-config コマンドを実行し、デバイス構成に NAT コマンドが存在するか評価することで、デバイスで NAT がアクティブになっているかどうかを確認できます。デバイスで NAT がアクティブになっている場合は、show running-config コマンドの出力に ip nat inside と ip nat outside インターフェイス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メッセージのNAT ALGのステータスを確認するには、管理者がデバイスにログインしてshow running-config | | include ip nat service rasコマンドを使用します。

```
<#root>

Router#

show running-config | include ip nat service ras


no ip nat service ras
Router#
```

上の例では、no ip nat service rasの出力で示されているように、H.323 RASメッセージに対してNAT ALGが無効になっています。

show running-config | | include ip nat service rasコマンドの出力に表示されているように、NAT ALGはH.323 RASメッセージに対して有効になっています。

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ログインして、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、その後ろに、Cisco IOS ソフトウェアのリリース番号とリリース名が表示されます。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します。

次に、Cisco IOS ソフトウェア リリース 15.5(2)T1 が実行されていて、インストールされているイメージ名が C2951-UNIVERSALK9-M であるデバイスでのコマンド出力例を示します。

```
<#root>

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関する詳細は、『White Paper: Cisco IOS and NX-OS Software Reference Guide』を参照してください。

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。

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メッセージでのNAT ALGの使用を無効にするには、グローバルコンフィギュレーションモードでno ip nat service rasコマンドを使用します。

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リリースしています。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、アクセスまたはその他の方法で使用した場合、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、[シスコのセキュリティアドバイザリおよびアラート (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 Cisco Service Contract 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 POS 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

お客様が Cisco IOS ソフトウェアの脆弱性による侵害の可能性を判断できるよう、シスコでは Cisco IOS Software Checker ツールを提供しています。このツールにより、特定の Cisco IOS ソフトウェア リリースに該当するシスコ セキュリティ アドバイザリ、および各アドバイザリで説明されている脆弱性が修正された最初のリリース（「First Fixed」）を特定できます。また該当する場合、そのリリースに関するすべてのアドバイザリ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入れたり、特定のアドバイザリのみ、または最新のバンドル資料のすべてのアドバイザリを含めるなど）を作成する

リリースが、公開されたシスコセキュリティアドバイザリのいずれかに該当するかどうかを確認するには、Cisco.comのCisco IOS Software Checkerを使用するか、以下のフィールドにCisco IOSソフトウェアリリース(たとえば、15.1(4)M2)を入力します。

オン

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）は、2022 年 3 月に、この脆弱性のさらなるエクスプロイトが試みられたことを認識しました。これらの脆弱性が修正済みのソフトウェアリリースにアップグレードすることを、引き続き強くお勧めします。

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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-nat

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	エクスプロイトに関する情報を更新。	不正利用事例と公式発表	Final	2022 年 12 月 16 日
1.0	初回公開リリース	—	Final	2017年9月27日

利用規約

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。