Cisco IOSソフトウェアのネットワークアドレス変換の脆弱性

アドバイザリーID : cisco-sa-20140326-nat
初公開日 : 2014-03-26 16:00
バージョン 1.0 : Final
CVSSスコア : 7.8
回避策 : No Workarounds available
Cisco バグ ID : CSCue00996 CSCuh33843 CSCuj41494

CVE-2014-2109
CVE-2014-2111

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ソフトウェアに実装されているネットワークアドレス変換(NAT)機能には、IPパケットの変換時に2つの脆弱性があり、認証されていないリモートの攻撃者によってサービス妨害(DoS)状態が引き起こされる可能性があります。

シスコはこれら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。これらの脆弱性を軽減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-20140326-nat

注： 2014年3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6件の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ています。各Cisco IOSソフトウェアセキュリティアドバイザリには、このアドバイザリで説明されている脆弱性を修正したCisco IOSソフトウェアリリースと、2014年3月のバンドル公開のすべてのCisco IOSソフトウェアの脆弱性を修正したCisco IOSソフトウェアリリースが記載されています。

個々の公開リンクは、次のリンクにある『Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication』に掲載されています。

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar14.html

該当製品

これらの脆弱性は、Cisco IOSソフトウェアの脆弱なバージョンを実行し、NATが設定されているデバイスに影響を与えます。

脆弱性のある製品

Cisco IOSソフトウェアを実行しているシスコデバイスは、NATが設定されている場合に脆弱性の影響を受けます。

デバイスにNATが設定されているかどうかを確認するには、次の2つの方法があります。

- デバイスでNATがアクティブかどうかを確認する
- 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

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には、デバイスでNATが有効になっているかどうかを確認することをお勧めします。

デバイスでNATがアクティブかどうかの確認

Cisco IOSソフトウェアの設定でNATが有効になっているかどうかを確認するには、デバイスにログインして show ip nat statisticsコマンドを発行します。NATがアクティブな場合、Outside interfacesと Inside interfacesのセクションに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ます。次の例は、NAT機能がアクティブになっているデバイスを示しています。<#root>

```
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
```

デバイスの設定にNATコマンドが含まれているかどうかの確認

また、Cisco IOSソフトウェアの設定でNATが有効になっているかどうかを判断するには、 ip nat insideコマンドと ip nat outsideコマンドが異なるインターフェイスに存在している必要が

あります。 NAT仮想インターフェイスの場合は、 ip nat enableインターフェイスコマンドが存在します。

注：デバイスに存在するCisco Easy VPNリモートクライアント機能の設定により、NATが自動的に有効になります。

Cisco Easy VPN Remote機能によって作成されたNATおよびポートアドレス変換(PAT)の設定は、スタートアップコンフィギュレーションファイルや実行コンフィギュレーションファイルには書き込まれません。ただし、これらの設定は、 show ip nat statisticsコマンドを使用して表示できます。

Cisco IOSソフトウェアリリースの判別

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て show version コマンドを使って、システム バナーを表示します。"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。

```
<#root>

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



!--- output truncated
```

Cisco IOSソフトウェアのリリース命名規則の追加情報は、『White Paper: Cisco IOS and NX-OS Software Reference Guide』で確認できます。

脆弱性を含んでいないことが確認された製品

NAT機能が設定されていないCisco IOSデバイスは脆弱ではありません。

次の製品には脆弱性が存在しないことが確認されています。

- 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ソフトウェアに実装されているネットワークアドレス変換(NAT)機能には、IPパケットの変換時に2つの脆弱性があり、認証されていないリモートの攻撃者によってサービス妨害(DoS)状態が引き起こされる可能性があります。

Cisco IOSソフトウェアのNAT DNSの脆弱性

Cisco IOSソフトウェアのApplication Layer Gateway(ALG)モジュールの脆弱性により、認証されていないリモートの攻撃者が該当デバイスのリロードを引き起こし、サービス妨害(DoS)状態が発生する可能性があります。

この脆弱性は、特定の不正なDNSパケットがネットワークアドレス変換(NAT)の対象となるデバイスで処理される方法に起因します。攻撃者は、不正なDNSパケットを送信して該当デバイスで処理および変換することにより、この脆弱性を不正利用する可能性があります。このエクスプロイトにより、攻撃者は該当システムのリロードを引き起こして、DoS 状態を発生させることができます。

この脆弱性は、IPv6パケットを使用して不正利用することはできません。この脆弱性は、ポート53を宛先とするTCPおよびUDPの両方のDNSパケットによって引き起こされる可能性があります。

この脆弱性は、該当デバイスを通過するトラフィックによってのみトリガーされ、該当デバイスを宛先とするトラフィックによって不正利用されることはありません。

この脆弱性は、Cisco Bug ID CSCue00996(登録ユーザ専用)として文書化され、CVE IDとしてCVE-2014-2111が割り当てられています

Cisco IOSソフトウェアのTCP入力の脆弱性

Cisco IOSソフトウェアのTCP入力モジュールの脆弱性により、認証されていないリモートの攻撃者が該当デバイスのメモリリークまたはリロードを引き起こし、サービス妨害(DoS)状態が発生する可能性があります。

この脆弱性は、該当デバイスでネットワークアドレス変換(NAT)が実行される際に、特定のTCPパケットシーケンスが処理される方法に起因します。攻撃者は、該当デバイスで処理される特定のTCPパケットシーケンスを送信することで、この脆弱性を不正利用する可能性があります。この不正利用により、攻撃者は該当デバイスのメモリリークまたはリロードを引き起こし、DoS状態を引き起こす可能性があります。

この脆弱性は、該当デバイスを通過するIPv6トラフィックによってトリガーされることはなく、該当デバイスを宛先とするトラフィックによって不正利用されることもありません。

この脆弱性により、該当するデバイスがリロードされる可能性がありますが、メモリリークが発生する可能性もあります。

該当するデバイスでこの脆弱性が不正利用され、メモリリークが確認されたかどうかを確認するには、コマンドラインインターフェイスから show memory debug leaks chunksコマンドを発行します。

次の例は、I/Oメモリ領域の IP Inputでメモリリークが確認された、該当するCisco IOSデバイスの出力を示しています。

```
Router#show memory debug leaks chunks
Adding blocks for GD...

                I/O memory


Address    Size   Alloc_pc  PID  Alloc-Proc       Name

Address    Size   Alloc_pc  PID  Alloc-Proc       Name
29ECB984   1252   23371C48  164  IP Input        *Packet Header*
```

注：IP Inputでのメモリリークは、他の多くの機能によって引き起こされる可能性があり、この脆弱性が不正利用されたことを示す明確なサインではありません。

注：show memory debug leaks chunks コマンドはCPUに負荷がかかる場合があるため、使用には注意が必要です。

この脆弱性は、Cisco Bug ID CSCuh33843（登録ユーザ専用）およびCSCuj41494（登録ユーザ専用）として文書化され、CVE IDとしてCVE-2014-2109が割り当てられています

回避策

Cisco IOSソフトウェアのTCP入力の脆弱性

この脆弱性に対する回避策はありません。

Cisco IOSソフトウェアのNAT DNSの脆弱性

この脆弱性は、外部IPアドレスのNAT変換のみの機能を設定することで軽減できます。

場合によっては、DNSパケットのペイロード部分のアドレスを変換できないことがあります。これには、DNSメッセージ内のアドレスを変更せずに残しておく必要があります。

これは、外部IPアドレスのNAT変換のみの機能を使用して実現されます。この機能は、ヘッダー部分のアドレスだけを変換しますが、ペイロード部分は変更しません。これは、変換されないアドレスとの通信が必要な場合に役立ちます。この機能を有効にするには、 ip nat inside source staticコマンドまたは ip nat outside source staticコマンドを no-payloadオプション付きで発行します。

修正済みソフトウェア

ソフトウェアのアップグレードを検討する場合は、 http://www.cisco.com/go/psirt のシスコ セキュリティ アドバイザリ、応答、および通知のアーカイブや、後続のアドバイザリを参照して侵害の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。

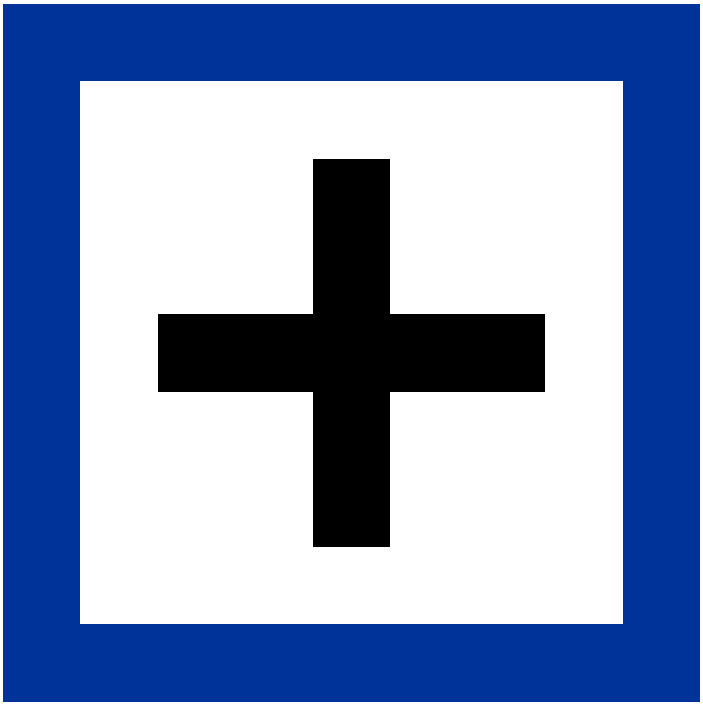
2014年2月、シスコは2005年から2010年の間に製造されたメモリコンポーネントに関する業界全体の問題の詳細を発表しました。これらのコンポーネントを使用するシスコ製品の大半で、フィールドでの故障率が予想レベルを下回っていますが、デバイスのリロードや電源の再投入によって、コンポーネントの障害が発生する可能性があります。この問題に関連する既知のセキュリティ上の影響はありませんが、影響を受ける製品のサブセットでは、ソフトウェアアップグレードプロセス中にメモリコンポーネントの障害が発生する可能性があります。アップグレードを決定する前に、関連情報と製品固有のField Notice(www.cisco.com/go/memory)を確認することを推奨します。各Field Noticeは、ソフトウェアのアップグレード中にメモリコンポーネントの障害が発生する可能性があるかどうかを示します。

Cisco IOS ソフトウェア

Cisco IOS Software Checkerは、Cisco IOSソフトウェアの脆弱性による影響を最も迅速に判断する方法です。 このツールを使用すると、特定のCisco IOSソフトウェアリリースに影響を与えるシスコセキュリティアドバイザリをすばやく特定できます。 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で、検索を開始できます。このツールでは、show versionコマンドの出力を解析することもできます。結果は、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、特定の資料、または2014年3月のバンドル資料のすべてのアドバイザリを検索してカスタマイズできます。

また、次のCisco IOSソフトウェアの表を使用して、問題の発生の有無を確認することもできます。 各行はCisco IOSソフトウェアリリースに対応しています。特定のリリースに脆弱性が存在する場合、その修正を含む最も古いリリースが2列目に表示されます。3列目には、この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のすべての脆弱性を修正する最初のリリースを記載しています。



展開して修正済みソフトウェアの詳細情報を表示

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、このアドバイザリで説明されている脆弱性の影響を受けません。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）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やその公表を確認していません。

Cisco IOSソフトウェアのNAT DNS脆弱性は、TACカスタマーサービスリクエストのトラブルシューティング中に発見されました。

Cisco IOSソフトウェアのTCP入力の脆弱性は、シスコの社内テストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140326-nat

改訂履歴

リビジョン 1.0	2014年3月26日	初回公開リリース

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。