Cisco IOS ソフトウェアの NAT64 機能で確認されたサービス妨害（DoS）の脆弱性

High

アドバイザリーID : cisco-sa-20190327-nat64

初公開日 : 2019-03-27 16:00

バージョン 1.0 : Final

CVSSスコア : 8.6

回避策 : No workarounds available

Cisco バグ ID : CSCvk61580

CVE-2019-1751

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 64（NAT64）機能に含まれる脆弱性により、認証されていないリモート攻撃者がインターフェイス キューのウェッジ状態またはデバイスのリロードを引き起こす可能性があります。

この脆弱性は、デバイスを介して送信される特定の IPv4 パケット ストリームの不適切な処理に起因します。 攻撃者は、デバイスを介して特定の IPv4 パケット ストリームを送信することによって、この脆弱性をエクスプロイトできる可能性があります。 エクスプロイトにより、攻撃者がインターフェイス キューのウェッジ状態またはデバイスのリロードを引き起こし、その結果サービス妨害（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ました。 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-20190327-nat64

このアドバイザリは、2019 年 3 月 27 日に公開された 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。このバンドルには、19 件の脆弱性に関して 17 件のシスコ セキュリティ アドバイザリが含まれています。 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： Cisco IOS および IOS XE ソフトウェアに関するセキュリティ アドバイザリ公開資料（半年刊、2019 年 3 月）

該当製品

脆弱性のある製品

この脆弱性は、該当する Cisco IOS ソフトウェアのリリースを実行し、NAT64（ステートレスまたはステートフル）、変換によるアドレスとポートのマッピング（MAP-T）、またはカプセル化によるアドレスとポートのマッピング（MAP-E）のいずれかが設定されたデバイスに影響を及ぼします。

脆弱性が存在する Cisco IOS ソフトウェア リリースの詳細については、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。

NAT64 設定の確認

管理者は、CLI で **show running-config | include nat64 enable|nat64 map-t|nat64 map-e** コマンドを使用することにより、NAT64（ステートレスまたはステートフル）、MAP-T、または MAP-Eのいずれかが設定されたデバイスを識別できます。 コマンドの出力結果に **nat64** が含まれている場合、デバイスに脆弱性が存在します。 次の例は、NAT64 が有効になっているデバイスでのコマンドの出力を示しています。

```
Router#show running-config | include nat64 enable|nat64 map-t|nat64 map-e
 nat64 enable
 nat64 enable
nat64 prefix stateless 2001:DB9:0:1::/96
nat64 route 192.1.1.0/24 GigabitEthernet0/1
Router#
```

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。

```
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、『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

このアドバイザリの脆弱性が存在する製品のセクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

シスコは、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を確認しました。

詳細

キュー ウェッジは、Cisco IOS または IOS XE ルータまたはスイッチで特定のパケットが受信されキューに入れられたものの、処理エラーのためキューから削除されないときに発生します。キュー ウェッジの詳細や Cisco IOS ソフトウェアでブロックされたインターフェイスを特定するために使用できる検出方法については、このアドバイザリの「回避策」セクションを参照してください。 シスコのセキュリティ ブログに記載されている「Cisco IOS Queue Wedges Explained」も参照してください。

エクスプロイトされた場合でも、エクスプロイト トラフィックの送信元を特定でき、かつこのトラフィックが脆弱なデバイスに継続して到達しないようにブロックできる場合、管理者がインターフェイスから CLI コンフィギュレーション コマンド **hold-queue <number> in** を入力することで、ルータがリロードされるまでの保持キューを増やせます。この例を、次に示します。

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#inte gigabitEthernet 1
Router(config-if)#hold
Router(config-if)#hold-queue 350 in
Router(config-if)#end
Router#
```

セキュリティ侵害の痕跡

デバイスがエクスプロイトされ、キューのウェッジ状態が発生する場合、入力キューのサイズが最大値より大きいインターフェイスが **show interface** コマンドの出力に表示されます。この例を、次に示します。

```
Router#show interface | include Input queue:
Input queue: 76/75/180/0 (size/max/drops/flushes); Total output drops: 0
```

回避策

この脆弱性に対処する回避策はありません。

この脆弱性におけるキー ウェッジのエクスプロイトは、次の方法で識別できます。

組み込みイベント マネージャ

脆弱性のある Cisco IOS デバイス上で、Tool Command Language（TCL）に基づく組み込みイベント マネージャ（EEM）ポリシーを利用すると、この脆弱性によって引き起こされたインターフェイス キュー ウェッジを識別して、検出することができます。 このポリシーによって、管理者は Cisco IOS デバイスのインターフェイスをモニタできるほか、インターフェイス入力キューがいっぱいになると、それを検出できます。 Cisco IOS EEM がこの脆弱性によるエクスプロイトの可能性を検出すると、それに反応してポリシーがネットワーク管理者にアラートを送信します。 それを受けて管理者は、入力キューをクリアするためにデバイスのアップグレード、適切な移行、またはリロードどの手段を行うか判断できます。

TCL スクリプトは、「Cisco Beyond: Embedded Event Manager (EEM) Scripting Community」（次のリンクでアクセス）からダウンロードできます。
https://supportforums.cisco.com/docs/DOC-19337

詳細については、シスコのセキュリティ ブログに記載されている「Cisco IOS Queue Wedges Explained」を参照してください。

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は新規リリースでも継続して適切なサポートが受けられることを確認してください。 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

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 リストからリリース（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** など）を入力します。

デフォルトでは、Cisco IOS ソフトウェアのチェックには、結果は、高セキュリティへの影響の

評価 (サー) または重大な脆弱性にのみが含まれています。 「中間」の SIR 脆弱性の結果を含めるには、Cisco.com の Cisco IOS ソフトウェア チェッカーを使用して、[Impact Rating] ドロップダウン リストの [中間（Medium）] チェックボックスをオンにします。

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

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190327-nat64

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.0	初回公開リリース		最終版	2019 年 3 月 27 日

利用規約