Cisco IOS XE ソフトウェアの DNS NAT プロトコル アプリケーション レイヤ ゲートウェイにおけるサービス妨害の脆弱性

アドバイザリーID : cisco-sa-alg-dos-hbBS7SZE
初公開日 : 2021-03-24 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 : CSCvv65113

CVE-2021-1446

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 XE ソフトウェアのネットワークアドレス変換（NAT）で使用される DNS アプリケーション レイヤ ゲートウェイ（ALG）機能における脆弱性により、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す可能性があります。

この脆弱性は、該当デバイスが特定の DNS パケットを検査する際に発生する論理エラーに起因します。攻撃者は、DNS パケットの NAT を実行する該当デバイスを介して、巧妙に細工された DNS パケットを送信することで、この脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功すると、攻撃者はデバイスのリロードを引き起こし、該当デバイスでサービス妨害（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。この脆弱性は、IPv6 トラフィック経由ではエクスプロイトできません。

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-alg-dos-hbBS7SZE

このアドバイザリは、2021 年 3 月に公開された 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。アドバイザリとリンクの一覧については、『Cisco Event Response: March 2021 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、Cisco IOS XE ソフトウェアの脆弱性が存在するリリースを実行し、NAT 処理用に設定されていて、DNS ALG 機能が有効になっているシスコデバイスに影響を及ぼします。 DNS ALG 機能は、デバイスで NAT が設定されるとすぐに有効になります。

NAT 設定の評価

1.デバイスがNATを実行するように設定されているかどうかを確認する

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できます。

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: 1 (0 static, 1 dynamic; 0 extended)
Outside interfaces:
  GigabitEthernet0/0/3


Inside interfaces:
  GigabitEthernet0/0/1
```

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。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。

2. NAT設定でDNS ALGが無効になっているかどうかを確認する

NAT 設定で DNS ALG が無効になっているかどうかを確認するには、show running-config | include ip nat service dns 特権 EXEC コマンドを使用します。no ip nat service dns tcp と no ip nat service dns udp の両方が、show running-config | include ip nat service dns コマンドの出力に存在する場合、DNS ALG は NAT 設定で無効になっています。

以下に、Cisco IOS XE ソフトウェアで L4R が構成されている場合の show running-config | include ip nat コマンドを、NAT 設定で DNS ALG が無効になっている Cisco IOS XE ソフトウェアで実行した場合の出力を示します。

<#root>

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


 no ip nat service dns tcp
 no ip nat service dns udp
```

no ip nat service dns tcp と no ip nat service dns udp の両方が show running-config | include ip nat service dns コマンドの出力に表示されず、デバイスで Cisco IOS XE ソフトウェアの影響を受けるバージョンが NAT が有効な状態で実行されている場合、その設定は脆弱です。

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のある製品セクションに記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- IOS ソフトウェア
- IOS XR ソフトウェア
- NX-OS ソフトウェア

回避策

この脆弱性に対処する回避策はありません。ただし、緩和策は使用できます。

管理者は、DNS パケットの NAT ALG を無効化することで、この脆弱性を緩和できる場合があります。ただし、該当デバイスを通じて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出ることがあり、その結果、通常のネットワークオペレーションが中断される可能性があります。

管理者は、この機能を無効化する前に、ネットワーク環境で DNS パケットの NAT ALG を使用する必要がないことを確認する必要があります。DNG パケットに対して NAT ALG の使用を無効化するには、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 service dns tcp および no ip nat service dns udp コマンドを使用できます。

この緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

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 セキュリティ アドバイザリ 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アップグレード ソリューション一式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（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

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 および IOS XE ソフトウェア

Cisco IOS ソフトウェアおよび IOS XE 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 Software Checker を提供しています。このツールにより、特定の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。

お客様は、Cisco Software Checker を使用して次の方法でアドバイザリを検索できます。

- ソフトウェアと 1 つ以上のリリースを選択します。
- 特定のリリースのリストを含む .txt ファイルをアップロードする
- show version コマンドの出力を入力する

検索を開始した後で、すべてのシスコ セキュリティ アドバイザリ、特定のアドバイザリ、または最新の公開資料に記載されているすべてのアドバイザリが含まれるように検索をカスタマイズできます。

また、次の形式を使用して、Cisco IOS または IOS XE ソフトウェアリリース（15.1(4)M2 や 3.13.8S など）を入力することで、そのリリースがシスコ セキュリティ アドバイザリの影響を受けているかどうかを判断できます。

Check

デフォルトでは、Cisco Software Checker の結果には、Security Impact Rating（SIR）が「重大」または「高」の脆弱性だけが含まれます。「中間」の SIR 脆弱性の結果を含めるには、Cisco.com にある Cisco Software Checker を使用して、検索をカスタマイズするときに [影響の評価（Impact Rating）] の下にある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。

Cisco IOS XE ソフトウェア リリースと Cisco IOS ソフトウェア リリースのマッピングについては、Cisco IOS XE ソフトウェアのリリースに応じて「Cisco IOS XE 2 Release Notes」、「Cisco IOS XE 3S Release Notes」、または「Cisco IOS XE 3SG Release Notes」を参照してください。

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。

出典

この脆弱性は Cisco TAC サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-alg-dos-hbBS7SZE

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2021 年 3 月 24 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。