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-KU9Z8kFX
初公開日 : 2022-09-28 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 : CSCwa78096

CVE-2022-20837

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 TCP 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、細工を施した 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、攻撃者がデバイスのリロードを引き起こし、影響を受ける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。

注：この脆弱性をエクスプロイトできるのは、該当デバイス経由で IPv4 TCP パケットを送信した場合のみです。この脆弱性は、IPv6 トラフィックを送信しても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-KU9Z8kFX

このアドバイザリは、2021 年 9 月に公開された Cisco IOS および IOS XE ソフトウェア 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 2022 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、TCP 用の DNS ALG 機能が有効になっている次の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。

- ASR 1000 シリーズ エンベデッド サービス プロセッサ モデル ESP 100-X と ESP 200-X
- Catalyst 8500 エッジ プラットフォーム モデル C8500-12X4QC と C8500-12X

脆弱性が存在する Cisco 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。

デバイス設定の確認

デバイスが NAT を実行するように設定されているかを確認する

NAT がデバイス上でアクティブかどうかを確認するには（推奨される方法）、管理者がデバイスにログインして、CLI で show ip nat statistics コマンドを実行します。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。

または、CLI で show running-config コマンドを発行し、デバイス構成に NAT コマンドが存在するかを評価します。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。

NAT 設定で TCP 用の DNS ALG が無効になっているかを確認する

NAT 設定で TCP 用の 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 が show running-config | include ip nat service dnsコマンドの実行結果に出力される場合は、NAT設定でTCPに対するDNS ALGが無効になっていることを意味します。

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 tcp 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。

- ASR 1000 シリーズ エンベデッド サービス プロセッサ モデル ESP 100、ESP 200、およびこれらより前のモデル
- Catalyst 8500 シリーズ エッジ プラットフォーム モデル C8500L-8S4X
- 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 TCP パケットに対して 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。管理者がグローバル コンフィギュレーション モードで no ip nat service dns tcp コマンドを実行すると、DNS パケットに対して NAT ALG の使用を無効化できます。

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。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

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。

Cisco.com の Cisco Support and Downloads ページには、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス (My Devices)] ツールを使用するお客

様のカスタマーデバイスサポート範囲も表示できます。

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

お客様が 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に、シスコは Cisco Software Checker を提供しています。このツールを使うことで、特定のソフトウェアリリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース（「First Fixed」）を特定できます。また、該当する場合には、Software Checker により判別されたすべてのアドバイザリに記載の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。

このツールを使用するには、「Cisco Software Checker」ページの手順に従います。あるいは、次のフォームを使用して、シスコ セキュリティ アドバイザリに該当するリリースであるかどうかを確認します。このフォームを使用するには、次の手順に従います。

1. ツールで検索するアドバイザリを選択します。このアドバイザリのみ、セキュリティ影響評価（SIR）が「重大」または「高」のアドバイザリのみ、すべてのアドバイザリのいずれかです。
2. リリース番号（15.9(3)M2、17.3.3 など）を入力します。
3. [チェック（Check）] をクリックします。

2		Critical,High,Medium
このアドバイザのみ		

Enter release number | Check

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-KU9Z8kFX

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	2022 年 9 月 28 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。