Cisco IOS XE ソフトウェアの NAT Session Initiation Protocol アプリケーション層ゲートウェイのサービス妨害（DoS）の脆弱性

アドバイザリーID : cisco-sa-20190925-sip-alg
CVE-2019-12646
初公開日 : 2019-09-25 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 : CSCvn65912

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）Session Initiation Protocol（SIP）アプリケーション層ゲートウェイ（ALG）の脆弱性により、認証されていないリモート攻撃者が影響を受ける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、NAT を実行時に、標的デバイスで一時的な SIP パケットが不適切に処理されることに起因します。SIP パケットの NAT を実行する標的デバイスに対して、細工した SIP パケットを UDP ポート 5060 経由で送信することで、エクスプロイトされ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、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-20190925-sip-alg

このアドバイザリは、2019 年 9 月 25 日に公開された Cisco IOS および IOS XE ソフトウェア リリースのセキュリティ アドバイザリ資料の一部です。この資料には、13 件の脆弱性に関する 12 件のシスコ セキュリティ アドバイザリが記載されています。アドバイザリとリンクの一覧については、『Cisco Event Response: September 2019 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

この脆弱性の影響を受けるのは、次のシスコ デバイスで脆弱性のある Cisco IOS XE ソフトウェア リリースを稼動し、また NAT 処理が設定されている場合です。

- Cisco 1100、4200、4300 Cisco Integrated Services Router（ISR; サービス統合型ルータ）
- Cisco Cloud Services Router（CSR）1000V シリーズ
- Cisco エンタープライズ ネットワーク コンピューティング システム（ENCS）
- シスコ サービス統合型仮想ルータ（ISRv）

注：SIP 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。

脆弱性が存在する Cisco IOS XE 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。

NAT 設定の検証

Cisco IOS XE ソフトウェアの設定で NAT が有効かどうかを判断するには、ip nat inside コマンドまたは ip nat outside コマンドが別のインターフェイスにあり、設定に少なくとも 1 つの ip nat グローバル コンフィギュレーション コマンドが必要です。また、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 が設定にあるかどうかを判断するには、脆弱性がある次の設定例に示すように show running-config | include ip nat コマンドを使用します。

<#root>

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


 ip nat inside
 ip nat outside
 ip nat inside source static 192.0.2.100 10.0.0.1
```

NAT 設定で SIP 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 特権 EXEC コマンドを使用します。no ip nat service が show running-config コマンドの出力に表示されない場合 | include ip nat の出力に存在する場合、SIP 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 構成において SIP 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


 ip nat inside
 ip nat outside
 ip nat inside source static 192.0.2.100 10.0.0.1 vrf sip
 no ip nat service sip udp port 5060
```

no ip nat service sip が show running-config コマンドの出力に表示されない場合 | include ip nat の出力に表示されず、デバイスが Cisco IOS XE ソフトウェアの影響を受けるバージョンを NAT が有効な状態で実行している場合、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 Cisco IOS ソフトウェア、Cisco IOS XR ソフトウェア、および 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。

セキュリティ侵害の痕跡

この脆弱性の不正利用に成功すると、該当するデバイスがリロードされ、crashinfo ファイルが生成されます。

この脆弱性が不正利用されているかどうかを確認するには、デバイスのスタック トレースをデコードして、スタック トレースと本脆弱性との関連性を確認します。

crashinfo ファイルを確認し、デバイスにこの脆弱性の不正利用が発生していないかを判別するには、Cisco Technical Assistance Center（TAC）までご連絡ください。

回避策

この脆弱性に対処する回避策はありません。

アップグレードが可能になるまでの間、管理者は対象デバイスを次のように設定することで、SIP ALG を無効化して脆弱性を緩和できます。

```
no ip nat service sip udp port 5060
```

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 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するため、シスコは Cisco IOS Software Checker ツールを提供しています。このツールを使用

すると、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。

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またはIOS XEソフトウェアリリース(たとえば、15.1(4)M2、3.13.8Sなど)を入力します。

Check

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。

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

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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-sip-alg

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	2019 年 9 月 25 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。