Cisco IOSおよびIOS XEソフトウェアのCisco Group Encrypted Transport VPNソフトウェアにおける境界外の書き込みの脆弱性

Medium

アドバイザリーID : cisco-sa-getvpn-rce-g8qR68sx　CVE-2023-20109
初公開日 : 2023-09-27 16:00
バージョン 1.0 : Final
CVSSスコア : 6.6
回避策 : No workarounds available
Cisco バグ ID : CSCwe14195 CSCwe24118 CSCwf49531

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ソフトウェアおよびCisco IOS XEソフトウェアのCisco Group Encrypted Transport VPN(GET VPN)機能の脆弱性により、グループメンバーまたはキーサーバの管理権限を持つ認証されたリモート攻撃者が、該当デバイスで任意のコードを実行したり、デバイスをクラッシュさせたりする可能性があります。

この脆弱性は、GET VPN機能のGroup Domain of Interpretation(GDOI)プロトコルおよびG-IKEv2プロトコルの属性の検証が不十分であることに起因します。攻撃者は、インストールされているキーサーバを侵害するか、攻撃者によって制御されるキーサーバを指すようにグループメンバーの設定を変更することで、この脆弱性を不正利用する可能性があります。不正利用に成功すると、攻撃者は任意のコードを実行して該当システムのフルコントロールを取得したり、該当システムのリロードを引き起こしたりして、サービス妨害(DoS)状態を発生させる可能性があります。詳細については、このアドバイザリの「詳細情報」のセクションを参照してください。

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-getvpn-rce-g8qR68sx

このアドバイザリは、Cisco IOSおよびIOS XEソフトウェアのセキュリティアドバイザリバンド

ル公開の2023年9月リリースの一部です。アドバイザリとリンクの一覧については、『Cisco Event Response: September 2023 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

公開時点では、この脆弱性は、Cisco IOSソフトウェアまたは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ていて、GDOIまたはG-IKEv2プロトコルが有効になっているシスコ製品に影響を与えました。

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

デバイスにGDOIまたはG-IKEv2プロトコルが設定され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 running-config | include crypto gdoi|gkm groupコマンドを使用します。

デバイスがCisco IOS XEソフトウェアを実行しており、GDOIプロトコルが設定されている場合、コマンドの出力例は次のようになります。

<#root>

```
Router#
show running-config | include crypto gdoi|gkm group


crypto gdoi group group1
Router#
```

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 XR ソフトウェア
- Meraki 製品
- NX-OS ソフトウェア

詳細

Cisco GET VPNは、Cisco IOSデバイスで発信またはCisco IOSデバイスを経由するプライベートWAN上のIPマルチキャストグループトラフィックまたはユニキャストトラフィックを保護するために必要な機能のセットです。GET VPNは、Group Key Management Protocol(GKMP)とIPsec暗号化を組み合わせて、IPマルチキャストまたはユニキャストトラフィックを保護する効率的な方法をユーザに提供します。

GDOIはInternet Key Exchange（IKE；インターネットキーエクスチェンジ）バージョン1(IKEv1)を使用します。GDOIに代わるG-IKEv2は、インターネットキーエクスチェンジバージョン2(IKEv2)プロトコルを実装し、GET VPNでIKEv2の利点を引き出せるようにします。

GDOIおよびG-IKEv2プロトコルは、グループメンバーと、承認されたグループメンバー間のセキュリティアソシエーションを確立するグループコントローラまたはキーサーバとの間で動作します。

シスコでは、この脆弱性が不正利用される可能性は2つの方法のいずれかであると考えています。どちらの方法でも、グループメンバーとキーサーバ間の通信は、相互に認証され認可された暗号化セッションを介して行われるため、環境への事前の侵入が必要になります。2つの方法は次のとおりです。

1. 攻撃者は既存のキーサーバを侵害し、キーサーバがグループメンバーに送信するGDOIまたはG-IKEv2パケットを変更できます。
2. 攻撃者は独自のキーサーバを構築してインストールし、攻撃者によって制御されるキーサーバと通信するようにグループメンバーを再設定します。この方法で不正利用するには、次の条件が満たされている必要があります。
    - 攻撃者は、制御されたキーサーバを指すようにグループメンバーを再設定する権限を持つ認証済みの管理ユーザとしてグループメンバーにログインします。
    - 制御キーサーバには、再構成されたグループメンバーと通信するための正しい事前共有キー(PSK)とポリシーが設定されています。
    - 制御キーサーバは、キーサーバがグループメンバーに送信するGDOIまたはG-IKEv2パケットを変更できます。

回避策

この脆弱性に対処する回避策はありません。

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。

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

シスコは、GET VPN機能の不正利用が試みられていることを検出し、この機能のテクニカルコードレビューを実施しました。この脆弱性はシスコの内部調査中に発見されました。これらの脆弱性が修正済みのソフトウェアリリースにアップグレードすることを、引き続き強くお勧めします。

出典

この脆弱性は、Cisco Advanced Security Initiatives Group(ASIG)のX. B.によって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-getvpn-rce-g8qR68sx

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	2023年9月27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。