Cisco IOSおよびIOS XEソフトウェアのインターネットキーエクスチェンジ(IKE)バージョン1フラグメンテーションにおけるDoS脆弱性

アドバイザリーID : cisco-sa-ikev1-NO2ccFWz
初公開日 : 2024-03-27 16:00
バージョン 1.0 : Final
CVSSスコア : 8.6
回避策 : Yes
Cisco バグ ID : CSCwh66334 CSCwf11183

CVE-2024-20308
CVE-2024-20307

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ソフトウェアのインターネットキーエクスチェンジバージョン1(IKEv1)フラグメンテーション機能の複数の脆弱性により、認証されていないリモートの攻撃者が該当システムでヒープオーバーフローまたは破損を引き起こす可能性があります。

これらの脆弱性の詳細については本アドバイザリの「詳細情報」セクションを参照してください。

シスコはこれら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。これらの脆弱性には、回避策が存在します。

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-ikev1-NO2ccFWz

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2024年3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: March 2024 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

これらの脆弱性は、Cisco IOSまたは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るシスコ製品に影響を与えます。次の条件の両方に当てはまります。

- IKEv1フラグメンテーションが有効である
- IKEv1に基づくすべてのタイプのVPNが設定されている

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。

CVE-2024-20307:この脆弱性を不正利用するには、デバイスでbuffers huge sizeコマンドを32,767より大きい値に設定する必要があります。

IKEv1フラグメンテーションの設定の決定

IKEv1フラグメンテーションが有効になっているかどうかを確認するには、show running-config | include crypto isakmp fragmentationコマンドを使用します。コマンドから何らかの出力が返された場合は、次の例に示すように、IKEv1フラグメンテーションが有効になっています。

<#root>

router#

show running-config | include crypto isakmp fragmentation

crypto isakmp fragmentation

デバイスのIKEv1設定の確認

IKEv1を使用する機能には、次のようなさまざまなタイプのVPNが含まれます。

- Dynamic Multipoint VPN（DMVPN）
- FlexVPN
- Group Encrypted Transport VPN（GET VPN）
- LAN 間 VPN
- リモート アクセス VPN（SSL VPN を除く）

デバイスでIKEv1が設定されているかどうかを確認するには、show ip socketsまたはshow udp EXECコマンドを使用することをお勧めします。デバイスでUDPポート500、UDPポート4500、またはUDPポート848(GDOI)が開いている場合、IKEv1パケットが処理されています。

次の例は、UDPポート500およびUDPポート4500でIPv4またはIPv6のいずれかを使用してIKEv1パケットを処理しているデバイスでのshow udpコマンドの出力を示しています。

<#root>

```
router#

show udp

Proto        Remote      Port      Local       Port  In Out  Stat TTY OutputIF
17        --listen--          192.168.130.21    500   0   0 1001011   0
17(v6)    --listen--          UNKNOWN           500   0   0 1020011   0
17        --listen--          192.168.130.21   4500   0   0 1001011   0
17(v6)    --listen--          UNKNOWN          4500   0   0 1020011   0
.
.
.
router#
```

バッファの巨大構成の判別(CVE-2024-20307でのみ必要)

バッファの巨大サイズがデフォルト値から変更されたかどうかを確認するには、show running-config | include buffers hugeコマンドを使用して、出力が返されることを確認します。次の例に示すように、コマンドの出力結果にバッファの大きいサイズの値が32,767を超えている場合、そのデバイスは脆弱であると見なされます。

<#root>

```
router#

show running-config | include buffers huge

buffers huge size 50000
```

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。

- 適応型セキュリティアプライアンスソフトウェア
- Firepower Threat Defense ソフトウェア
- IOS XR ソフトウェア
- Meraki 製品
- NX-OS ソフトウェア

詳細

これらの脆弱性は依存関係にはなく、いずれかの脆弱性をエクスプロイトするために、他の脆弱性をエクスプロイトする必要はありません。また、いずれかの脆弱性の影響を受けるリリースであっても、他の脆弱性の影響は受けない場合があります。

脆弱性の詳細は以下のとおりです。

CVE-2024-20308:Cisco IOSおよびIOS XEソフトウェアのIKEv1フラグメンテーションヒープアンダーフローにおけるDoS脆弱性

Cisco IOSソフトウェアおよびCisco IOS XEソフトウェアのIKEv1フラグメンテーションコードの脆弱性により、認証されていないリモートの攻撃者がヒープアンダーフローを引き起こし、その結果デバイスのリロードが発生する可能性があります。

この脆弱性は、巧妙に細工されたフラグメント化されたIKEv1パケットが適切に再構成されないことに起因しています。攻撃者は、巧妙に細工されたUDPパケットを該当システムに送信することにより、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者が該当デバイスをリロードできるようになり、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。

注：この脆弱性は、該当システム宛てのトラフィックによってのみ不正利用が可能です。また、この脆弱性は、IPv4 トラフィックと IPv6 トラフィックでトリガーされ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。本脆弱性に対処する回避策がいくつかあります。

バグID:CSCwh66334
CVE ID：CVE-2024-20308
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：8.6
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

CVE-2024-20307:Cisco IOSおよびIOS XEソフトウェアのIKEv1フラグメンテーションヒープオーバーフローにおけるDoS脆弱性

Cisco IOSソフトウェアおよびCisco IOS XEソフトウェアのIKEv1フラグメンテーションコードの脆弱性により、認証されていないリモートの攻撃者がヒープオーバーフローを引き起こし、結果として該当デバイスのリロードが発生する可能性があります。

この脆弱性は、巧妙に細工されたフラグメント化されたIKEv1パケットが適切に再構成されないことに起因しています。攻撃者は、巧妙に細工されたUDPパケットを該当システムに送信することにより、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、攻撃者は該当デバイスのリロードを引き起こし、その結果 DoS 状態が発生する可能性があります。

注：この脆弱性は、該当システム宛てのトラフィックによってのみ不正利用が可能です。また、この脆弱性は、IPv4 トラフィックと IPv6 トラフィックでトリガーされ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。本脆弱性に対処する回避策がいくつかあります。

バグID:CSCwf11183
CVE ID：CVE-2024-20307
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.8
CVSSベクトル：CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:H

回避策

CVE-2024-20308：この脆弱性に対処する回避策があります。IKEv1フラグメンテーションを無効にします。

IKEv1フラグメンテーションを無効にするには、次の例のコマンドを使用します。

<#root>

```
Router# configure terminal
Router(config)#

no crypto isakmp fragmentation


Router(config)#end
Router#
```

CVE-2024-20307：この脆弱性に対処する回避策があります。バッファの巨大な設定をデフォルト値に戻すか、IKEv1フラグメンテーションを無効にします。

次の例のコマンドを使用して、バッファの巨大設定をデフォルト値に戻します。

<#root>

```
Router# configure terminal
Router(config)#

default buffers huge size


Router(config)#end
Router#
```

IKEv1フラグメンテーションを無効にするには、次の例のコマンドを使用します。

<#root>

```
Router# configure terminal
Router(config)#

no crypto isakmp fragmentation


Router(config)#end
Router#
```

IKE v1フラグメンテーション機能により、大きなIKEパケットを一連のより小さなIKEパケットにフラグメント化し、UDPレイヤでのフラグメント化を回避できます（たとえば、大きな証明書ペイロードや証明書要求ペイロードの場合）。ステートフルパケットインスペクションが設定されているファイアウォールなど、一部のサードパーティベンダーのデバイスでは、UDPフラグメントがフラグメント化攻撃の一部である場合に備えて、これらのフラグメントのパススルーが許可されません。

これらの回避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 シスコサポート & ダウンロードページには、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 | オン

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

CVE-2024-20307は、Cisco Advanced Security Initiatives Group(ASIG)のX. B.による内部セキュリティテストで発見されました。

CVE-2024-20308は、Cisco Advanced Security Initiatives Group(ASIG)による内部セキュリティテストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ikev1-NO2ccFWz

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	2024年3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。