Cisco IOS および IOS XE ソフトウェアのインターネット キー エクスチェンジにおけるメモリ リークの脆弱性

High

アドバイザリーID : cisco-sa-20180328-ike CVE-2018-0158
初公開日 : 2018-03-28 16:00
最終更新日 : 2022-12-15 22:19
バージョン 1.1 : Final
CVSSスコア : 8.6
回避策 : No workarounds available
Cisco バグ ID : CSCvf22394

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2(IKEv2)モジュールの脆弱性により、認証されていないリモート攻撃者が該当デバイスのメモリリークまたは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。

この脆弱性は、特定の IKEv2 パケットの不適切な処理に起因します。影響を受けるデバイスでは、巧妙に細工された IKEv2 パケットが送信されると、本脆弱性が不正利用される可能性があります。不正利用に成功すると、該当デバイスがメモリを消費し続け、最終的にリロードが引き起こされ、その結果、DoS 状態にな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-20180328-ike

このアドバイザリは、2018年3月28日に公開された22件の脆弱性に関する20件のシスコセキュリティアドバイザリを含む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 2018 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 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、Internet Security Association and Key Management Protocol（ISAKMP）が有効になっているシスコ デバイスに影響を与えます。

脆弱性が存在する Cisco IOS ソフトウェアおよび IOS XE ソフトウェアの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」の項を参照してください。

この脆弱性の原因となり得るものはIKEv2パケットに限られます。Cisco IOSソフトウェアまたはCisco IOS XEソフトウェアを実行するデバイスでは、ISAKMPが有効になっていると脆弱性が発生します。デバイスでは、脆弱性が存在する IKEv2 固有の機能を設定する必要はありません。デバイスに IKEv1 または IKEv2 が設定されている場合に、本脆弱性の影響がおよびます。どちらの場合でも、不正なパケットが処理されるためです。

IKE は、次に示すさまざまな VPN タイプを含む、多くの機能で使用されます。

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

IKE が有効かどうかの確認

デバイスで IKE が設定されているか確認するには、管理者は CLI で show ip sockets または show udp EXEC コマンドを使用します。UDP ポート 500、UDP ポート 848、UDP ポート 4500、UDP ポート 4848 のいずれかがデバイスでオープンされている場合、そのデバイスは IKE パケットを処理しています。

次の例は、UDP ポート 500 および UDP ポート 4500 で IKE 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ます。このデバイスでは、IP バージョン 4（IPv4）または IP バージョン 6（IPv6）を使用しています。

```
<#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#
```

Cisco IOS ソフトウェア リリースの判別

デバイス上で実行されている Cisco IOS ソフトウェア リリースは、管理者がデバイスにログインして、CLI で show version コマンドを使用し、表示されるシステム バナーを参照することにより確認できます。デバイスが Cisco IOS ソフトウェアを実行している場合、システム バナーに「Cisco Internetwork Operating System Software」や「Cisco IOS Software」などのテキストが表示されます。バナーにはインストールされたイメージ名もカッコ内に表示され、その後ろに、Cisco IOS ソフトウェアのリリース番号とリリース名が表示されます。一部のシスコ デバイスでは、show version コマンドをサポートしていなかったり、別の出力が表示されたりします。

次に、Cisco IOS ソフトウェア リリース 15.5(2)T1 が実行されていて、インストールされているイメージ名が C2951-UNIVERSALK9-M であるデバイスでのコマンド出力例を示します。

<#root>

```
Router>
```

show version

```
Cisco IOS Software, C2951 Software (C2951-UNIVERSALK9-M), Version 15.5(2)T1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Mon 22-Jun-15 09:32 by prod_rel_team
.
.
.
```

Cisco IOS ソフトウェア リリースの命名と番号付けの規則に関する詳細は、『Cisco IOS and NX-OS Software Reference Guide』を参照してください。

Cisco IOS XE ソフトウェア リリースの判別

デバイス上で実行されている Cisco IOS XE ソフトウェア リリースは、管理者がデバイスにログインして、CLI で show version コマンドを実行し、表示されるシステム バナーを参照することにより確認できます。デバイスが Cisco IOS XE ソフトウェアを実行している場合、システム バナーに「Cisco IOS Software」、「Cisco IOS XE Software」などのテキストが表示され

ます。

次に、Cisco IOS XR ソフトウェア リリース 16.2.1 が実行されていて、インストールされているイメージ名が CAT3K_CAA-UNIVERSALK9-M であるデバイスでのコマンドの出力例を示します。

<#root>

```
ios-xe-device#
show version

Cisco IOS Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version Denali 16.2.1, REL
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Sun 27-Mar-16 21:47 by mcpre
.
.
.
```

Cisco IOS XE ソフトウェア リリースの命名と番号付けの規則に関する詳細は、『Cisco IOS and NX-OS Software Reference Guide』を参照してください。

脆弱性を含んでいないことが確認された製品

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

シスコは、この脆弱性が Cisco IOS XR ソフトウェアまたは 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。

詳細

IKEv2 プロトコルは IPsec プロトコル スイートで暗号属性のネゴシエーションに使用され、この属性は暗号化または通信セッションの認証に使用されます。これらの属性には暗号化のアルゴリズム、モード、共有キーが含まれます。IKE ネゴシエーションの結果得られる共有セッション秘密が、暗号キーを導出するために使用されます。

Cisco IOSソフトウェアおよびCisco IOS XEソフトウェアは、IPv4およびIPv6通信用のIKEv2をサポートします。IKEv2 通信は次の UDP ポートを使用できます。

- UDP ポート 500
- UDP ポート 848、Group Domain of Interpretation（GDOI）
- UDP ポート 4500、ネットワーク アドレス変換トラバーサル（NAT-T）
- UDP ポート 4848、GDOI NAT-T

この脆弱性の原因となり得るものは IKEv2 パケットに限られます。ISAKMP が有効な場合、IKEv2 は Cisco IOS および IOS XE ソフトウェアで自動的に有効になります。

攻撃者が、IPv4 または IPv6 で上記リストの UDP ポートのいずれかを使用し、この脆弱性を不正利用する可能性があります。

セキュリティ侵害の痕跡

本脆弱性を不正利用すると、GKM GM プロセスによるメモリ リークが発生する可能性があります。次の例では、5 番目の列の値が増加しており、メモリ リークの兆候が示されています。これは本脆弱性に起因する可能性があります。

```
<#root>

Router#

show processes memory | include GKM GM Process

 440   0   13127152        448

13156648

         64    48 GKM GM Process
Router#

show processes memory | include GKM GM Process

 440   0   13130192        448

13159688

         64    48 GKM GM Process
Router#

show processes memory | include GKM GM Process

 440   0   13134192        448

13163688

         64    48 GKM GM Process
Router#
```

set memory debug incremental starting-time が定義された状態で show memory debug incremental leaks コマンドを実行した場合、メモリ リークを示す兆候は次の例のように表示されます。

```
<#root>

Router#

show memory debug incremental leaks
```

```
Adding blocks for GD...
lsmpi_io memory
Address    Size   Alloc_pc  PID  Alloc-Proc       Name
Processor memory
Address          Size     Alloc_pc  PID  Alloc-Proc      Name
7FD007DC81E0      352 55A8A4DED6D0  434  Crypto IKE Disp gkm packet
7FD007DC8340      160 55A8A4DB3E63  440  GKM GM Process  reverse addr
7FD007DC83E0      400 55A8A4DB3968  434  Crypto IKE Disp GKM Rekey / Ack Packet Container
7FD007DC8570      352 55A8A4DED6D0  434  Crypto IKE Disp gkm packet
7FD007DC86D0      144 55A8A4DEDB4E  434  Crypto IKE Disp GKM Queue Data
7FD007DC8760      160 55A8A4DB3E63  440  GKM GM Process  reverse addr
7FD007DC8800      400 55A8A4DB3968  434  Crypto IKE Disp GKM Rekey / Ack Packet Container
7FD007DC8990      352 55A8A4DED6D0  434  Crypto IKE Disp gkm packet
7FD007DC8AF0      144 55A8A4DEDB4E  434  Crypto IKE Disp GKM Queue Data
7FD007DC8B80      160 55A8A4DB3E63  440  GKM GM Process  reverse addr
7FD007DC8C20      400 55A8A4DB3968  434  Crypto IKE Disp GKM Rekey / Ack Packet Container
7FD007DC8DB0      352 55A8A4DED6D0  434  Crypto IKE Disp gkm packet
```

攻撃が進行中の場合、エントリ数は増加し続けることが予測されます。

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

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ソフトウェアまたはCisco 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。

オン

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、2022 年 3 月に、この脆弱性のさらなるエクスプロイトが試みられたことを認識しました。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 TAC のサポート要求の対応中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-ike

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	エクスプロイトに関する情報を更新。	不正利用事例と公式発表	Final	2022年12月15日
1.0	初回公開リリース	—	Final	2018年3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。