

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 Denial of Service (DoS) の脆弱性

High アドバイザリーID : cisco-sa-20170927-ike [CVE-2017-12237](#)
初公開日 : 2017-09-27 16:00
バージョン 1.0 : Final
CVSSスコア : [8.6](#)
回避策 : Yes
Cisco バグ ID : [CSCvc41277](#)

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影響を受けるデバイスでの CPU 大量消費、トレースバック メッセージ、またはリロードを引き起こし、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。

この脆弱性は、特定の IKEv2 パケットを処理する方法に起因します。影響を受けるデバイスでは、特定の IKEv2 パケットが送信されると脆弱性がエクスプロイトされる可能性があります。エクスプロイトが成功すると、攻撃者が影響を受けるデバイスでの CPU 大量消費、トレースバック メッセージ、またはリロードを引き起こし、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。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。この脆弱性に対処する回避策はありません。

このアドバイザリーは、次のリンクより確認できます。

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-ike>

このアドバイザリーは、2017 年 9 月 27 日に公開された 13 件の脆弱性に関する 12 件のシスコ セキュリティ アドバイザリーを含む 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 アドバイザリー バンドルの一部です。これらのアドバイザリーとリンクの一覧については、以下を参照してください。[シスコのイベント対応 : Cisco IOS および IOS XE ソフトウェアに関するセキュリティ アドバイザリー公開資料 \(半年刊、2017 年 9 月 \)](#)

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 を有効にす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。

IKEv2 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

デバイスが IKE のために設定されたかどうかを判別する好まれる方法は CLI の `show ip sockets` が `show udp EXEC` コマンドを発行することです。UDP ポート 500、UDP ポート 848、または UDP ポート 4500 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。

次の例では、デバイスが、IPv4 または IPv6 のどちらかを使用して 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ことを示しています。

```
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ガイ

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ます。その後ろには Cisco IOS ソフトウェアのリリース番号とリリース名も表示されます。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することがあります。

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。

```
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ついては、以下を参照してください。[ホワイト ペーパー：Cisco IOS および NX-OS ソフトウェア リファレンス ガイド](#)

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。

```
ios-xe-device# show version
```

```
Cisco IOS Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version Denali 16.2.1, RELEASE SOFTWARE (fc1)
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ついては、以下を参照してください。[ホワイト ペーパー：Cisco IOS および NX-OS ソフトウェア リファレンス ガイド](#)

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。

また、シスコは、この脆弱性が Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス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 ソフトウェアでは、IPv4 および IPv6 通信用 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)

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 ソフトウェアおよび Cisco IOS XE ソフトウェアで ISAKMP を有効にすると IKEv2 は自動的に有効になります。これらの脆弱性が発生するのは、IKEv2 パケットが送信された場合に限られます。

本脆弱性をエクスプロイトは、リストに掲載された UDP ポートのいずれかにおいて、IPv4 と IPv6 のどちらかを使用して起きる可能性があります。

セキュリティ侵害の痕跡

利用されたプラットフォームとエクスプロイトにより、侵害状況は異なります。影響を受けるデバイスでの CPU の大量消費、トレースバック メッセージ、リロードなどが引き起こされ、DoS 状態が発生する可能性があります。

この脆弱性で Crypto IKEv2 プロセスによる CPU の大量消費が生じる可能性があります。次に、この脆弱性によって引き起こされる可能性がある CPU 大量消費の例を示します。

```
Router# sh proc cpu sorted
```

```
CPU utilization for five seconds: 99%/6%; one minute: 64%; five minutes: 52%
PID Runtime(ms)      Invoked      uSecs   5Sec   1Min   5Min  TTY Process
PID Runtime(ms)      Invoked      uSecs   5Sec   1Min   5Min  TTY Process
```

```
391      2949388      188131      15677 83.72% 53.79% 43.27% 0 Crypto IKEv2
```

この脆弱性によって引き起こされるトレースバックメッセージには、Crypto IKEv2 プロセスの CPUHOG が記録されます。次に、この脆弱性によって引き起こされる可能性があるトレースバックメッセージの例を示します。

```
Router# sh proc cpu sorted
```

```
CPU utilization for five seconds: 99%/6%; one minute: 64%; five minutes: 52%
```

```
PID Runtime(ms)      Invoked      uSecs   5Sec   1Min   5Min TTY Process
PID Runtime(ms)      Invoked      uSecs   5Sec   1Min   5Min TTY Process
391      2949388      188131      15677 83.72% 53.79% 43.27% 0 Crypto IKEv2
```

この脆弱性によりデバイスがリロードされた場合、Crypto IKEv2 プロセスによってリロードが引き起こされたことを示すメッセージが表示されます。次の例は、デバイスのリロードがこの脆弱性に起因することを示しています。

```
Router# sh proc cpu sorted
```

```
CPU utilization for five seconds: 99%/6%; one minute: 64%; five minutes: 52%
```

```
PID Runtime(ms)      Invoked      uSecs   5Sec   1Min   5Min TTY Process
PID Runtime(ms)      Invoked      uSecs   5Sec   1Min   5Min TTY Process
391      2949388      188131      15677 83.72% 53.79% 43.27% 0 Crypto IKEv2
```

回避策

デバイスサポートのソフトウェア リリースがこのコマンドを使用する暗号 `ikev2` 制限キュー `sainit` 設定コマンド (Ciscoバグ [CSCvc12306](#) を参照して下さい) 修正済みリリースとアップグレードの実行と同等なら。これ以外に、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 アップデートを提供しています。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、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、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です。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、[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 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

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、シスコでは [Cisco IOS Software Checker](#) ツールを提供しています。このツールにより、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、すべてのアドバイザリに記載された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。

このツールを使用して次のタスクを実行できます。

- ドロップダウンメニューからリリース (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含めたり、特定のアドバイザリのみ、または最新のバンドル資料から全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。

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) では、本アドバイザリに記載されている脆弱性のエクスプロイト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 のサポート ケースの解決中に発見されました。

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-ike>

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2017 年 9 月 27 日

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。

本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。