# Cisco IOS Software and IOS XE Software Internet Key Exchange Version 2 Denial of Service Vulnerabilities

High

**アドバイザリーID :** cisco-sa-20150325-ikev2

**初公開日 :** 2015-03-25 16:00

**最終更新日 :** 2016-12-07 17:03

**バージョン 1.3 :** Final

**CVSSスコア :** 7.8

**回避策 :** No workarounds available

**Cisco バグ ID :** CSCum36951 CSCuo75572

CVE-2015-0642

CVE-2015-0643

**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 ソフトウェアまたは IOS XE ソフトウェアを実行するデバイスでは、インターネット キー エクスチェンジ（IKE）バージョン 2 サブシステム内の脆弱性から影響を受けます。認証されていないリモート攻撃者からサービス妨害（DoS）を受ける危険性があります。

本脆弱性は、特定の不正な 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、不正な 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、該当システムがリロードされたり、過剰なリソース消費により DoS 状態が引き起こされたりする危険性があります。 Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアを実行するデバイスで Internet Security Association and Key Management Protocol（ISAKMP）を有効にすると、IKEv2 は自動的に有効になります。 本脆弱性が発生するのは、不正な IKEv2 パケットが送信された場合に限られます。

このアドバイザリに記載されている脆弱性に対する回避策はありません。 シスコはこれらの脆弱性に対処するソフトウェア アップデートを提供しています。

このアドバイザリは、次のリンクより確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-ikev2

**注: 2015 年 3 月 25 日、Cisco IOS ソフトウェアおよび IOS XE ソフトウェアのセキュリティ ア**

**ドバイザリにおいて、7 つの Cisco Security Advisory を含むバンドル資料を公開しました。 これらのアドバイザリは Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアの脆弱性を扱っています。 個々の公表資料へのリンクは、次のリンクにある「*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 アドバイザリ公開資料*」に掲載されています。**

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar15.html

### 該当製品

## 脆弱性のある製品

本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、IKEv1 または ISAKMP を有効にすると脆弱性が発生します。

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
- Group Encrypted Transport VPN（GETVPN）

IKE がデバイスに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 コマンドを使用します。 デバイスの UDP ポート 500 または UDP ポート 4500 が開放されている場合、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、IP バージョン 4（IPv4）または IP バージョン 6（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
!--- Output truncated
router#
```

また、Cisco IOS ソフトウェアは、GETVPN の G-IKEv2 機能を有効にした場合に、IPv4 または IPv6 を使用して UDP ポート 848（GDOI）上で IKE パケットを処理します。

シスコ製品上で動作している Cisco IOS ソフトウェア リリースについては、管理者がデバイスにログインして **show version** コマンドを発行し、システム バナーを表示することで判別できます。 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た場合は、デバイスが Cisco IOS ソフトウェアを実行しています。 カッコ内にイメージ名が表示され、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続きます。 他のシスコ デバイスでは、**show version** コマンドが存在しなかったり、別の出力が表示されたりします。

次の例は、Cisco IOS ソフトウェア リリースが 15.2(4)M5、インストールされたイメージ名が C3900-UNIVERSALK9-M であるシスコ製品を示しています。

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.2(4)M5, RELEASE SOFTWARE
(fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Fri 13-Sep-13 16:44 by prod_rel_team
```

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.2(4)M5, RELEASE SOFTWARE
(fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Fri 13-Sep-13 16:44 by prod_rel_team
```

Cisco IOS ソフトウェア リリースの命名規則については、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

Cisco IOS XR は、これらの脆弱性の影響を受けません。

Cisco NX-OS は、これらの脆弱性の影響を受けません。

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。

## 詳細

IKEv2 プロトコルは IP Security（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 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 4500、ネットワーク アドレス変換（NAT）トラバーサル（NAT-T）
- UDP ポート 848、G-IKEv2 for GETVPN を有効にした場合の Group Domain of Interpretation（GDOI）

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の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。

本脆弱性は、特定の不正な 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、不正な 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。このエクスプロイトにより、攻撃者は該当システムのリロードを引き起こして、DoS 状態を発生させることができます。

Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアで IKEv1 または 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、不正な IKEv2 パケットが送信された場合に限られます。

エクスプロイトされると、影響を受けるデバイスのリロードまたはメモリ枯渇が引き起こされ、DoS 状態につながる可能性があります。

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。

脆弱性の内容は以下に文書化されています。

- Cisco Bug ID CSCuo75572（登録ユーザ専用）、Common Vulnerabilities and Exposures（CVE）ID CVE-2015-0643 が割り当てられています。
- Cisco Bug ID CSCum36951（登録ユーザ専用）、Common Vulnerabilities and Exposures（CVE）ID CVE-2015-0642 が割り当てられています。

## 回避策

これらの脆弱性を軽減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場合は、 http://www.cisco.com/go/psirt の Cisco Security Advisories, Responses, and Alerts アーカイブや、後続のアドバイザリを参照して侵害の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。

### Cisco IOS ソフトウェア

シスコでは、Cisco IOS ソフトウェアの脆弱性にさらされているかどうかを判断するためのツールを提供しています。 Cisco IOS Software Checker により、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を選択するか、ローカル システムからファイルをアップロードすることによって、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、特定の資料のみ、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

このツールを使うことで、そのソフトウェア 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、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。 Cisco IOS Software Checker を参照するか、次のフィールドに Cisco IOS ソフトウェア リリースを入力して、いずれかの公開された Cisco IOS ソフトウェア アドバイザリに該当するかどうかを判断できます。

（入力例： 15.1(4)M2）

## Cisco IOS XE ソフトウェア

| Cisco IOS XE ソフトウェア リリース | First Fixed Release（修正された最初のリリース） | 2015 年 3 月 の Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドル パブリケーションのすべてのアドバイザリに対する First Fixed Release（修正された最初のリリース） |
|---|---|---|
| 2.5.x | 脆弱性あり; 3.12.3S 以降へ移行 | 脆弱性あり; 3.12.3S 以降へ移行 |
| 2.6.x | 脆弱性あり; 3.12.3S 以降へ移行 | 脆弱性あり; 3.12.3S 以降へ移行 |
| 3.1.xS | 脆弱性あり; 3.12.3S 以降へ移行 | 脆弱性あり; 3.12.3S 以降へ移行 |
| 3.1.xSG | 脆弱性なし | 脆弱性なし |
| 3.2.xS | 脆弱性あり; 3.12.3S 以降へ移行 | 脆弱性あり; 3.12.3S 以降へ移行 |
| 3.2.xSE | 脆弱性あり; migrate to 3.7.1E or later. | 脆弱性あり; migrate to 3.7.1E or later. |
| 3.2.xSG | 脆弱性なし | 脆弱性なし |

| | | |
|---|---|---|
| 3.2.xXO | 脆弱性なし | 脆弱性なし |
| 3.2.xSQ | 脆弱性なし | 脆弱性なし |
| 3.3.xS | 脆弱性あり; 3.12.3S 以降へ移行 | 脆弱性あり; 3.12.3S 以降へ移行 |
| 3.3.xSE | 脆弱性あり; migrate to 3.7.1E or later. | 脆弱性あり; migrate to 3.7.1E or later. |
| 3.3.xSG | 脆弱性あり; migrate to 3.7.1E or later. | 脆弱性あり; migrate to 3.7.1E or later. |
| 3.3.xXO | 脆弱性あり; migrate to 3.7.1E or later. | 脆弱性あり; migrate to 3.7.1E or later. |
| 3.3.xSQ | 脆弱性なし | 脆弱性なし |
| 3.4.xS | 脆弱性あり; 3.12.3S 以降へ移行 | 脆弱性あり; 3.12.3S 以降へ移行 |
| 3.4.xSG | 脆弱性あり; migrate to 3.7.1E or later. | 脆弱性あり; migrate to 3.7.1E or later. |
| 3.4.xSQ | 脆弱性なし | 脆弱性なし |
| 3.5.xS | 脆弱性あり; 3.12.3S 以降へ移行 | 脆弱性あり; 3.12.3S 以降へ移行 |
| 3.5.xE | 脆弱性あり; migrate to 3.7.1E or later. | 脆弱性あり; migrate to 3.7.1E or later. |
| 3.6.xS | 脆弱性あり; 3.12.3S 以降へ移行 | 脆弱性あり; 3.12.3S 以降へ移行 |
| 3.6.xE | 脆弱性あり; migrate to 3.7.1E or later. | 脆弱性あり; migrate to 3.7.1E or later. |
| 3.7.xS | 脆弱性あり; 3.12.3S 以降へ移行 | 脆弱性あり; 3.12.3S 以降へ移行 |
| 3.7.xE | 3.7.1E | 3.7.1E |
| 3.8.xS | 脆弱性あり; 3.12.3S 以降へ移行 | 脆弱性あり; 3.12.3S 以降へ移行 |
| 3.9.xS | 脆弱性あり; 3.12.3S 以降へ移行 | 脆弱性あり; 3.12.3S 以降へ移行 |
| 3.10.xS | 3.10.5S | 脆弱性あり; 3.12.3S 以降へ移行 |
| 3.11.xS | 脆弱性あり; 3.12.3S 以降へ移行 | 脆弱性あり; 3.12.3S 以降へ移行 |
| 3.12.xS | 3.12.3S | 脆弱性あり; 3.12.3S 以降へ移行 |
| 3.13.xS | 3.13.2S | 3.13.2S |
| 3.14.xS | 脆弱性なし | 脆弱性なし |

| | | |
|---|---|---|
| 3.15.xS | 脆弱性なし | 脆弱性なし |

Cisco IOS ソフトウェア リリースへの Cisco IOS XE ソフトウェア リリースのマッピングについては、「Cisco IOS XE 2 Release Notes」、「Cisco IOS XE 3S Release Notes」、および「Cisco IOS XE 3SG Release Notes」を参照してください。

## Cisco IOS XR ソフトウェア

Cisco IOS XR ソフトウェアは、2015 年 3 月の Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドルに含まれている脆弱性の影響を受けません。

## 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。

これらの脆弱性は、内部テストおよび Cisco TAC によるカスタマー ケースの解決中に発見されました。

## 出典

## URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-ikev2

## 改訂履歴

| Version | Description | Section | Status | 日付 |
|---|---|---|---|---|
| 1.3 | Updated OVAL definitions are available. | | | 2016-December-07 |
| 1.2 | 過去に公開されたすべてのCisco IOSソフトウェア セキュリティ アドバイザリを照会できる Cisco IOS Checker ソフトウェアの Checker フォームを更新しました。 | | | 2016 年 1 月 14 日 |
| 1.1 | 2015 年 3 月 の Cisco IOS ソフトウェア セキュリティ アドバイザリ バンドル パブリケーションのすべてのアドバイザリにおいて First Fixed Release（修正した最初のリリース）の箇所を更新しました。 | | | 2015 年 3 月 25 日 |
| 1.0 | 初回公開リリース | | | 2015 年 3 月 25 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、単独の転載や意訳を施した場合、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。