Cisco IOS および IOS XE ソフトウェア Internet Key Exchange（IKE）バージョン 2 フラグメンテーション サービス拒否の脆弱性

High

アドバイザリーID : cisco-sa-20160323-ios-ikev2

初公開日 : 2016-03-23 16:00

バージョン 1.0 : Final

CVSSスコア : 7.1

回避策 : No workarounds available

Cisco バグ ID : CSCux38417

CVE-2016-1344

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 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 2（v2）フラグメンテーション コードの脆弱性はリモート攻撃者非認証により影響を受けたシステムのリロードを引き起こすようにする可能性があります。

脆弱性は巧妙に細工されたの、フラグメント化された IKEv2 パケットの不適当な処理が原因です。 攻撃者は影響を受けたシステムへ巧妙に細工された UDP パケットを送信 することによってこの脆弱性を不正利用する可能性があります。 エクスプロイトは攻撃者により影響を受けたシステムのリロードを引き起こすことを可能にする可能性があります。

注: 本脆弱性を不正利用する目的で使用できるのは、該当システム宛てのトラフィックに限られます。 この脆弱性は IPv4 および IPv6 トラフィックによって引き起こすことができます。

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-20160323-ios-ikev2

このアドバイザリは、6 脆弱性を記述する 6 Cisco Security Advisory を含む Cisco IOS および IOS XE ソフトウェア Security Advisory によって組み込まれる書のリリースの 2016 年 3月 23 日一部です。 すべての脆弱性にあります「最高のセキュリティ へ の 影響 定格が」。 それらへのアドバイザリおよびリンクの完全なリストに関しては、 Cisco イベント応答が表示されて下さい : 半年ごと Cisco IOS および IOS XE ソフトウェア Security Advisory によって組み込まれる書。

該当製品

この脆弱性は Cisco IOS または Cisco IOS XE ソフトウェアの脆弱なバージョンを実行する製品に影響を及ぼします。 Cisco IOS および IOS XE ソフトウェア リリースが脆弱である詳細については、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下さい。

脆弱性のある製品

実行するデバイスはソフトウェアの脆弱なバージョン次の 2 つの条件が確認される場合影響を受けています:

- IKEv2 フラグメンテーションは有効に なります
- デバイスは Cisco IOS か Cisco IOS XE ソフトウェアを実行して、IKEv2 に基づいて VPN のあらゆる型のために設定されます

注: IKEv1-based VPN はこの脆弱性から影響を受けません; ただし、場合によっては、IKEv1 を有効に することは自動的に IKEv2 を有効に します。

いくつかの機能は次のような VPN の異なる型を含む IKEv2 を、使用します:

- 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）

IKEv2 フラグメンテーションが有効に なるかどうか確かめるために、 **show running-config を**使用して下さい **| 暗号 ikev2 フラグメンテーション コマンドを含み、**出力を戻すことを確認して下さい。

次の例はデバイス示したものです Cisco IOSソフトウェアを有効に なる *暗号 ikev2* フラグメンテーションと動作します:

```
router#show running-config | include crypto ikev2 fragmentation
crypto ikev2 fragmentation
```

注: IKEv2 フラグメンテーションはデフォルトで有効に なりません。

デバイスが IKEv2 のために設定されたかどうか判別する好まれる方法は **show ip sockets** か **show udp** EXEC コマンドを発行することです。 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 running-config | include crypto ikev2 fragmentation
```

```
crypto ikev2 fragmentation
```

Cisco IOSソフトウェアはまた IPv4 か IPv6 を使用して GETVPN のための G-IKEv2 機能が有効に なった場合、UDP ポート 848 （ GDOI ）の IKE パケットを、処理します。

Cisco IOS か Cisco IOS XE ソフトウェア バージョンの判別

、管理者はデバイスにログインどの Cisco IOS ソフトウェア リリースが Cisco製品で動作しているか判別し、**show version コマンドを**コマンドラインインターフェイスで使用し、次に現われるシステムバナーを参照するためにできます。 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。 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。

次の例は、Cisco IOS ソフトウェア リリースが 15.5(2)T1 で、インストールされたイメージ名が *C2951-UNIVERSALK9-M* であるシスコ製品を示しています。

```
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]

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。

詳細

セキュリティ侵害の痕跡

回避策

IKEv2 フラグメンテーションは **暗号 ikev2 フラグメンテーション コマンドの**使用なによってディセーブルにすることができます。

IKEv2 フラグメンテーションが必要である場合、この脆弱性を軽減する回避策がありません。

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。
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.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場合は、http://www.cisco.com/go/psirt の Cisco Security Advisories and Responses アーカイブや後続のアドバイザリを参照して、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は新規リリースでも継続して適切なサポートが受けられることを確認してください。 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 Technical Assistance Center（TAC）に連絡してアップグレードを入手してください。
http://www.cisco.com/en/US/support/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

顧客が Cisco IOS および IOS XE ソフトウェアの脆弱性への公開を判別するのを助けるために Cisco はツールを、各アドバイザリに説明がある脆弱性を解決する以前のリリースおよび特定のソフトウェア リリースに影響を与える Cisco Security Advisory を識別する Cisco IOSソフトウェア チェッカー提供します、（「最初に」固定される）。 該当する場合、ツールはまた以前のリリースを戻します識別されるすべてのアドバイザリに説明があるすべての脆弱性を解決する（「結合される最初に」固定される）。

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

リリースがあらゆる公開された Cisco Security Advisory から影響を受けするかどうか判別するために、Cisco.com の Cisco IOSソフトウェア チェッカーを使用するか、または—次のフィールドで… Cisco IOS か IOS XE ソフトウェア リリースを—たとえば、**15.1(4)M2** か **3.01.4S** 入力して下さい:

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

この問題はデイヴィッド Barksdale、ヨルダン Gruskovnjak、および出国知性のアレックス荷車引きによって報告された関連 問題の調査の間に見つけられました。

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160323-ios-ikev2

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2016-March-23

利用規約