Cisco IOS および IOS XE ソフトウェア Internet Key Exchange（IKE）バージョン 1 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-20160928-ios-ikev1

初公開日 : 2016-09-28 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 : CSCuy47382

CVE-2016-6381

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 Internet Key Exchange（IKE）バージョン 1（IKEv1）フラグメンテーション コードの脆弱性は非認証、リモート攻撃者により利用可能なメモリの枯渇か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。

脆弱性は巧妙に細工されたの、フラグメント化された IKEv1 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。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-ios-ikev1

このアドバイザリは、2016 年 9 月 28 日に公開された 11 件の脆弱性に関する 10 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。 このすべての脆弱性はセキュリティへの影響が「高」と評価されています。 これらのアドバイザリ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 アドバイザリ公開資料（半年刊、2016 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なリリースを実行する製品に影響を及ぼします。 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。

実行するデバイスはソフトウェアの脆弱なリリース次の 2 つの条件が確認される場合影響を受けています。 IKEv1 フラグメンテーションがデフォルトでイネーブルになっていないことに注目して下さい。

- IKEv1 フラグメンテーションはイネーブルになっています
- デバイスは Cisco IOSソフトウェアか Cisco IOS XE ソフトウェアを実行して、IKEv1 に基づいて VPN のあらゆる型のために設定されます

いくつかの機能は次のような VPN の異なる型を含む IKEv1 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）

IKEv1 フラグメンテーションがイネーブルになってい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 isakmp 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 IKEv1 フラグメンテーションがイネーブルの状態で動作します:

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

デバイスが IKEv1 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 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ソフトウェアはまた IPv4 か IPv6 を使用して UDP ポート 848 （ GDOI ）の IKE パケットを、処理します。

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、コマンドライン インターフェイス (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]

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 XE Software*」などのテキストが表示されます。

次に、Cisco IOS XE ソフトウェア リリース 3.16.1aS が実行されているデバイスでの **show version** コマンドの出力例を示します。

```
Router> show version
Cisco IOS XE Software, Version 03.16.01a.S - Extended Support Release
Cisco IOS Software, ASR1000 Software (PPC_LINUX_IOSD-ADVENTERPRISEK9-M), Version 15.5(3)S1a,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Wed 04-Nov-15 17:40 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。

回避策

IKEv1 フラグメンテーションは **暗号 isakmp 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。 IKEv1 フラグメンテーションが必要である場合、この脆弱性に対処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 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

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**、**3.1.4S** 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

この脆弱性は内部テストで発見されました。

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-ios-ikev1

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2016 年 9 月 28 日

利用規約