複数のシスコ製品の IKEv1 情報漏洩の脆弱性

High

アドバイザリーID : cisco-sa-20160916-ikev1

初公開日 : 2016-09-16 16:00

最終更新日 : 2016-10-05 15:09

バージョン 1.3 : Interim

CVSSスコア : 7.8

回避策 : No workarounds available

Cisco バグ ID : CSCvb36055 CSCvb29204

CVE-2016-6415

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

Internet Key Exchange（IKE）Cisco IOS、Cisco IOS XE および Cisco IOS XR ソフトウェアのコードを処理するバージョン 1（IKEv1）パケットの脆弱性は非認証が、リモート攻撃者 機密 情報の公開の原因となる可能性があるメモリ内容を取得するようにする可能性があります。

脆弱性は不充分な条件が原因チェックインします IKEv1 セキュリティ ネゴシエーション要求を処理するコードの一部をです。 攻撃者は設定された影響を受けたデバイスへ巧妙に細工された IKEv1 パケットを送信 することによって IKEv1 セキュリティ ネゴシエーション要求を受け入れるためにこの脆弱性を不正利用する可能性があります。 正常なエクスプロイトは攻撃者が機密 情報の公開の原因となる可能性があるメモリ内容を取得することを可能にする可能性があります。

シスコでは、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する予定です。 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-20160916-ikev1

該当製品

Cisco IOS XR ソフトウェア

Cisco IOS XR ソフトウェアの次のリリースを実行するすべての製品はこの脆弱性から影響を受けます:

- Cisco IOS XR 4.3.x

- Cisco IOS XR 5.0.x
- Cisco IOS XR 5.1.x
- Cisco IOS XR 5.2.x

Cisco IOS XR ソフトウェア リリース 5.3.x はおよびより新しいこの脆弱性から影響を受けしません。

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。

注: 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 Cisco IOS の該当するリリースの調査の結果をアップデートし、Cisco IOS XE ソフトウェアおよび結果は特定のソフトウェア リリースおよび諮問それぞれに説明がある脆弱性を解決する以前の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 チェッカーを通して利用できます、（「最初に」固定される）。

シスコでは現在、この脆弱性の影響を受ける製品とそれらの製品への各影響を特定するために、製品ラインを調査中です。 調査の進捗に応じて、シスコは該当する各製品の Cisco Bug ID など、本アドバイザリ内の情報を更新します。 Cisco Bug Search Tool を使用するとバグを検索でき、利用可能な回避策や修正されたソフトウェア リリースなど、プラットフォーム固有の追加情報を入手できます。

脆弱性のある製品

Cisco は IKE バージョン 1 （IKEv1）を使用するために設定されるとき以下の製品が脆弱であることを判別しました:

- Cisco IOSソフトウェアの該当するリリースを実行するすべてのシスコ製品
- Cisco IOS XE ソフトウェアの該当するリリースを実行するすべてのシスコ製品
- Cisco IOS XR ソフトウェアの該当するリリースを実行するすべてのシスコ製品
- Cisco PIX ファイアウォール

注: IKEv1 パケットだけこの脆弱性を誘発するのに使用することができるが Cisco IOSソフトウェアか Cisco IOS XE ソフトウェアを実行しているデバイスは IKEv1 か IKEv2 を使用するために設定されるとき脆弱です。

調査は進行中その他のCisco製品がこの脆弱性から影響を受けるかもしれなかったかどうか確認するためにです。 このセクションは追加製品が脆弱であるために確認されている場合更新済です。

注: Cisco はこの問題を調査し、ことを PIXバージョン 6.x この脆弱性から前に影響を受けます結論し。

PIXバージョン 7.0 およびそれ以降はこの脆弱性によって変化しないために確認されます。 Cisco PIX は 2009 年以来サポートされないし、サポートされていませんでした。

IKEv2 IOS software か Cisco IOS XE ソフトウェアを on Cisco 設定することは自動的に IKEv1 を有効に します。

IKEv1 または IKE バージョン 2 （IKEv2）が設定されるとき IKEv1 が on Cisco 自動的にイネーブルになられていた IOS software および Cisco IOS XE ソフトウェアであるが、脆弱性は巧妙に細工された IKEv1 パケットの送信によってだけことができます引き起こす。

いくつかの機能は異なる VPN を含む IKEv1 を、使用します（以下を参照）:

- LAN 間 VPN
- リモート アクセス VPN（SSL VPN を除く）
- Dynamic Multipoint VPN（DMVPN）
- グループ ドメイン オブ インタープリテーション（GDOI）

注: Cisco IOS XR プラットフォームは DMVPN か GDOI ベースの VPN をサポートしません。

デバイスが IKE のために設定されたかどうか確認する 2 つの方式があります:

- IKE ポートが実行デバイスで開いていたかどうか確認して下さい
- IKE 機能がデバイスコンフィギュレーションに含まれていたかどうか確認して下さい

IKE ポートが実行デバイスで開いていたかどうか確認して下さい

デバイスが IKE のために設定されたかどうか確認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。 デバイスが UDP ポート 500、UDP ポート 4500、UDP ポート 848、または開いた UDP ポート 4848 を備えていれば IKE パケットを処理しています。

次の例では、デバイスは IPv4 か IPv6 を使用して UDP ポート 500 および UDP ポート 4500 の IKE パケットを、処理しています:

```
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#
```

IKE 機能がデバイスコンフィギュレーションに含まれていたかどうか確認して下さい

Cisco IOSデバイス設定が脆弱だったかどうか確認するために、管理者は IKE を使用する少なくとも 1 つの設定された特性があるかどうか確かめる必要があります。 これを **show run** の使用によって達成することができます **| クリプト マップを含んで下さい|保護 ipsec をトンネル伝送して下さい|暗号 gdoi** enable mode コマンド。 このコマンドの出力が *クリプト マップ*、 *トンネル保護 ipsec*、または *暗号 gdoi* が含まれていれば、デバイスは IKE 設定が含まれています。 次の例は IKE のために設定されたデバイスを示したものです:

```
router# show run | include crypto map|tunnel protection ipsec|crypto gdoi
crypto map CM 100 ipsec-isakmp
 crypto map CM
router#
```

注: IKEv1 SA ネゴシエーション要求を受け入れるシスコ製品だけこの脆弱性から影響を受けます。 デバイスが IKE 主要で、積極的でかまたは速いモード Security Association （SA）確立を始めるかまたは IKE および IPSec SA のための鍵変更を始めれば、この脆弱性によって不正利用することができません。 IKEv1 SA ネゴシエーションだけを始める Ciscoデバイスはこの脆弱性から影響を受けません。

注: Cisco Easy VPN （EzVPN）クライアントコンフィギュレーションはまだ IKE 要求を聞き取り、そのような要求の処理によって不正利用することができます。

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** コマンドを使用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 3.6.2S (Cisco IOS ソフトウェア リリース 15.2(2)S2 にマッピング) 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 Software, IOS-XE Software (PPC_LINUX_IOSD-ADVENTERPRISEK9-M), Version 15.2(2)S2,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Tue 07-Aug-12 13:40 by mcpre
```

Cisco IOS XR 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 XR ソフトウェア リリースとそれを実行しているデバイスの名前は、管理者がデバイスにログインして、CLI で **show version** コマンドを使用することにより確認できます。 デバイスが Cisco IOS XR 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 XR Software* 」などのテキストが表示されます。 デバイスで現在実行しているシステム イメージ ファイルの場所と名前は、「 *System image file is*」の横に表示

されます。 ハードウェア製品の名前はシステム イメージ ファイル名の次の行に表示されます。

次に、Cisco IOS XR ソフトウェア リリース 4.1.0 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 *mbihfr-rp.vm* であるデバイスでの **show version** コマンドの出力例を示します。

```
RP/0/RP0/CPU0:router# show version
 Mon May 31 02:14:12.722 DST

 Cisco IOS XR Software, Version 4.1.0
 Copyright (c) 2010 by Cisco Systems, Inc.

 ROM: System Bootstrap, Version 2.100(20100129:213223) [CRS-1 ROMMON],

 router uptime is 1 week, 6 days, 4 hours, 22 minutes
 System image file is "bootflash:disk0/hfr-os-mbi-4.1.0/mbihfr-rp.vm"

 cisco CRS-8/S (7457) processor with 4194304K bytes of memory.
 7457 processor at 1197Mhz, Revision 1.2
```

脆弱性を含んでいないことが確認された製品

Cisco ASA 5500 および Cisco ASA 5500-X シリーズはこの脆弱性から適応型セキュリティ アプライアンス（ASA）ソフトウェア影響を受けません。

調査は進行中その他のCisco製品がこの脆弱性から影響を受けるかもしれなかったかどうか確認するためにです。 このセクションはより多くの詳細として学習されますアップデートされます。

他の製品は現在この公開の時にこの脆弱性から影響を受けるために知られていません。

詳細

インターネット プロトコル セキュリティ（IPsec）プロトコル スイートで IKE プロトコルがコミュニケーションのセッションを暗号化するか、または認証するのに使用する暗号属性をネゴシエートするのに使用されています。 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 の最終結果は暗号化キーを得るのに使用する共用セッション シークレットです。

IPv4 および IPv6 通信のための Cisco IOS、Cisco IOS XE および Cisco IOS XR ソフトウェア サポート IKE。 IKE 通信はの次の UDP ポート使用できます:

- UDP ポート 500
- UDP ポート 4500、NAT 走査（NAT-T）
- UDP ポート 848、Group Domain of Interpretation（GDOI）
- UDP ポート 4848、GDOI NAT-T

コード IOS、Cisco IOS XE および Cisco IOS XR を on Cisco 処理する IKEv1 パケットの脆弱性は非認証が、リモート攻撃者 機密 情報の公開の原因となる可能性があるメモリ内容を取得するようにす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。 この脆弱性は IKEv1 のために設定されるデバイスによって処理される IKEv1 トラフィックによってしか不正利用することができません。 中継 IKEv1 トラフィックはこの脆弱性を誘発できません。 IKEv2 は影響を受けていません。

不正利用する可能性があるパケットのスプーフィングはこの脆弱性脆弱なデバイスから最初の応答に受け取るか、またはアクセスできる攻撃者が必要があるので限られています。

セキュリティ侵害の痕跡

Cisco IPS シグニチャは 7699-0 および Snort SID 40220(1)、40221(1)、および 40222(1) この脆弱性を不正利用する試みを検出できます。

回避策

この脆弱性に対する回避策はありません。

管理者はこの脆弱性を不正利用するように試みる不正侵入を検出し、防ぐのを助けるように侵入防御システム（IPS）か intrusion detection system （IDS）を設定するために助言されます。

管理者は影響を受けたシステムを監視するように助言されます。

修正済みソフトウェア

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。

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。

さらに、顧客は彼らに有効なライセンスがある Cisco から、または Cisco 認定再販業者かパートナーを通して直接手に入れられるソフトウェア ダウンロードだけかもしれないです。 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。

不正利用事例と公式発表

2016 年 8月 15 日で、同等化グループからの公開を所有するように要求したシャドウ仲介商グループ オンラインで掲示された Cisco は情報に警告 されました。 掲示された資料はマルチプルベンダーからのファイアーウォール製品のためのエクスプロイトが含まれていました。 技術情報はレガシー Cisco PIXファイアウォールを不正利用するのに可能性としては使用される BENIGNCERTAIN エクスプロイトに関する情報が含まれていました。

シャドウ仲介商公開に基づいて、Cisco は BENIGNCERTAIN と同じような脆弱性によって影響を与えることができる他の製品の調査を開始しました。

Cisco製品のセキュリティ上の問題に対する回答チーム (PSIRT) は影響を受けたプラットフォームを実行している何人かの Cisco カスタマ向けの脆弱性の不正利用に気づいています。

出典

この脆弱性のエクスプロイトは Cisco PIX のための疑わしいシャドウ仲介商グループ公に表われました。

シャドウ仲介商公開に基づいて、Cisco は BENIGNCERTAIN と同じような脆弱性によって影響を与えることができる他の製品の調査を開始しました。

脆弱性 on Cisco IOS、Cisco IOS XE および Cisco IOS XR は Cisco 内の内部 保全テスト チームによって見つけられました。

URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160916-ikev1

改訂履歴

Version	Description	Section	Status	日付
1.3	該当製品および脆弱性が存在する製品セクションをアップデートしました。	該当製品および脆弱性のある製品	Interim	2016-October-05
1.2	Affected Products セクションをアップデートしました。	該当製品	Interim	2016-September-20
1.1	Affected Products セクションをアップデートしました。	該当製品	Interim	2016-September-19
1.0	初回公開リリース		Interim	2016-September-16

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。