複数のシスコ製品における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

Cisco IOS、Cisco IOS XE、およびCisco IOS XR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1(IKEv1)パケット処理コードの脆弱性により、認証されていないリモート攻撃者がメモリの内容を取得し、機密情報が漏洩する可能性があります。

この脆弱性は、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における不十分な条件チェックに起因します。攻撃者は、IKEv1セキュリティネゴシエーション要求を受け入れるように設定された該当デバイスに、巧妙に細工されたIKEv1パケットを送信することにより、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、メモリの内容を搾取できるようになり、機密情報の漏洩につなが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。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160916-ikev1

該当製品

Cisco IOS XR ソフトウェア

次のCisco IOS XRソフトウェアリリースを実行しているすべての製品が、この脆弱性の影響を受けます。

- Cisco IOS XR 4.3.x
- Cisco IOS XR 5.0.x（販売終了）
- Cisco IOS XR 5.1.x
- Cisco IOS XR 5.2.x（販売終了）

Cisco IOS XRソフトウェアリリース5.3.x以降は、この脆弱性の影響を受けません。

Cisco IOS および IOS XE ソフトウェア

お客様が 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するため、シスコは Cisco IOS Software Checker ツールを提供しています。このツールを使用すると、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、そのリリースに関する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。

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入れたり、特定のアドバイザリのみ、または最新のバンドル資料のすべてのアドバイザリを含めるなど）を作成する

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リリースであるかどうかを確認するには、Cisco.com の Cisco IOS ソフトウェアチェッカーを使用するか、以下のフィールドに Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェアのリリース番号（たとえば、15.1(4)M2、3.1.4S など）を入力します。

Check

注：お客様がCisco IOSソフトウェアおよびIOS XEソフトウェアの脆弱性の影響を受ける可能性があるかどうかを判断できるように、シスコは該当するCisco IOSソフトウェアおよびCisco IOS XEソフトウェアのリリースの調査結果を更新し、その結果を Cisco IOS Software Checkerで確認できるようにします。このツールは、特定のソフトウェアリリースに影響するシスコセキュリティアドバイザリと、各アドバイザリで説明されている脆弱性をを修正する最初のリリース（「最初の」）を修正したものです。

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

シスコでは、IKEバージョン1(IKEv1)を使用するように設定されている次の製品には脆弱性が存在すると判断しています。

- 影響を受けるCisco IOSソフトウェアリリースを実行しているすべてのシスコ製品
- 影響を受けるCisco IOS XEソフトウェアリリースを実行しているすべてのシスコ製品
- 影響を受けるCisco IOS XRソフトウェアリリースを実行しているすべてのシスコ製品
- Cisco PIX ファイアウォール

注：この脆弱性の原因となり得るものはIKEv1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は、IKEv1またはIKEv2を使用するように設定されている場合、脆弱性の影響を受けます。

他のシスコ製品がこの脆弱性の影響を受ける可能性があるかどうかを判断するため、現在調査中です。このセクションは、追加の製品に脆弱性が存在することが判明した場合に更新されます。

注：シスコはこの問題を調査し、PIXバージョン6.x以前がこの脆弱性の影響を受けると結論付けました。

PIXバージョン7.0以降は、この脆弱性の影響を受けないことが確認されています。Cisco PIXは2009年からサポートされておらず、サポートされていません。

Cisco IOSソフトウェアまたはCisco IOS XEソフトウェアでIKEv2を設定すると、自動的にIKEv1が有効になります。

Cisco IOSソフトウェアおよびCisco IOS XEソフトウェアでは、IKEv1またはIKEバージョン2(IKEv2)が設定されるとIKEv1が自動的に有効になりますが、この脆弱性は巧妙に細工されたIKEv1パケットを送信することによってのみ引き起こされます。

IKEv1は、次のようなさまざまなVPN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）
- Group Domain of Interpretation（GDOI；グループドメイン通訳）

注：Cisco IOS XRプラットフォームは、DMVPNまたはGDOIベースのVPNをサポートしてい

ません。

デバイスにIKEが設定されているかどうかを確認するには、次の2つの方法があります。

- 実行中のデバイスでIKEポートが開いているかどうかを確認する
- デバイスの設定にIKE機能が含まれているか確認する

実行中のデバイスでIKEポートが開いているか確認する

デバイスにIKEが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。デバイスでUDPポート500、UDPポート4500、UDPポート848、またはUDPポート4848が開放されている場合、IKEパケットが処理されています。

次の例では、デバイスはIPv4またはIPv6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ます。

<#root>

```
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#
```

デバイス設定にIKE機能が含まれているか確認する

Cisco IOSデバイスの設定が脆弱かどうかを判断するには、管理者は、IKEを使用する機能が1つ以上設定されているかどうかを確認する必要があります。これは、 show run | include crypto map|tunnel protection ipsec|crypto gdoi enable modeコマンドを使用します。このコマンドの出力に crypto map、 tunnel protection ipsec、 crypto gdoiのいずれかが含まれている場合は、デバイスにIKE設定が含まれています。次の例は、IKEが設定されているデバイスを示しています。

<#root>

router#

show run | include crypto map|tunnel protection ipsec|crypto gdoi

```
crypto map CM 100 ipsec-isakmp
 crypto map CM
router#
```

注： この脆弱性の影響を受けるのは、IKEv1 SAネゴシエーション要求を受け入れるシスコ製品のみです。デバイスがIKEのメイン、アグレッシブ、またはクイックモードのセキュリティアソシエーション(SA)の確立を開始する場合、またはIKEおよびIPSec SAのキー再生成を開始する場合、この脆弱性によって不正利用されることはありません。 IKEv1 SAネゴシエーションのみを開始するシスコデバイスは、この脆弱性の影響を受けません。

注：Cisco Easy VPN(EzVPN)クライアントの設定はまだIKE要求をリッスンしているため、このような要求を処理することで不正利用される可能性があります。

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、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します。

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。

```
<#root>

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関する詳細は、『White Paper: Cisco IOS and NX-OS Software Reference Guide』を参照してください。

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。

<#root>

```
Router#

show version

Cisco IOS Software, IOS-XE Software (PPC_LINUX_IOSD-ADVENTERPRISEK9-M), Version 15.2(2)S2, RELEASE SO
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。

<#root>

```
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シリーズ適応型セキュリティアプライアンスはこの脆弱性の影響を受けません。

他のシスコ製品がこの脆弱性の影響を受ける可能性があるかどうかを判断するため、現在調査中です。このセクションは、詳細が学習された時点で更新されます。

このアドバイザリが公開された時点で、他にこの脆弱性の影響を受ける製品は現在確認されていません。

詳細

IKEプロトコルは、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、通信セッションの暗号化または認証に使用される暗号属性のネゴシエーションに使用されます。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の最終的な結果は、暗号キーを導出するために使用される共有セッションシークレットです。

Cisco IOS、Cisco IOS XE、およびCisco IOS XRソフトウェアは、IPv4およびIPv6通信用のIKEをサポートしています。IKE通信では、次のUDPポートのいずれかを使用できます。

- UDP ポート 500
- UDPポート4500、NATトラバーサル(NAT-T)
- UDP ポート 848、Group Domain of Interpretation（GDOI）
- UDP ポート 4848、GDOI NAT-T

Cisco IOS、Cisco IOS XE、およびCisco IOS XRのIKEv1パケット処理コードの脆弱性により、認証されていないリモート攻撃者がメモリの内容を取得し、機密情報が開示され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。この脆弱性の不正利用が可能なのは、IKEv1用に設定されたデバイスによって処理されているIKEv1トラフィックのみです。通過するIKEv1トラフィックはこの脆弱性を引き起こしません。IKEv2は影響を受けません。

この脆弱性を不正利用する可能性のあるパケットのスプーフィングは、攻撃者が脆弱なデバイスから最初の応答を受信するか、その応答にアクセスする必要があるため、制限されます。

セキュリティ侵害の痕跡

Cisco IPSシグニチャ7699-0およびSnort SID 40220(1)、40221(1)、および40222(1)は、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。

この脆弱性を悪用しようとする攻撃を検出して防止するために、侵入防御システム(IPS)または侵入検知システム(IDS)を実装することをお勧めします。

影響を受けるシステムをモニタすることを推奨します。

修正済みソフトウェア

Cisco IOS および IOS XE ソフトウェア

お客様が 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するため、シスコは Cisco IOS Software Checker ツールを提供しています。このツールを使用すると、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、そのリリースに関する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。

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入れたり、特定のアドバイザリのみ、または最新のバンドル資料のすべてのアドバイザリを含めるなど）を作成する

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リリースであるかどうかを確認するには、Cisco.com の Cisco IOS ソフトウェアチェッカーを使用するか、以下のフィールドに Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェアのリリース番号（たとえば、15.1(4)M2、3.1.4S など）を入力します。

Check

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。こ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、アクセス、またはその他の方法で使用する場合、お客様はシスコのソフトウェアライセンス(

http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html)の条項に従うことに同意したことになります。

また、お客様がソフトウェアをダウンロードできるのは、有効なライセンスを保有しており、シスコから直接、またはシスコ認定の再販業者もしくはパートナーを通じて購入したソフトウェアに限られます。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)(http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html)に連絡してアップグレードを入手してください。

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。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

2016年8月15日、シスコはShadow Brokersグループがオンラインで投稿した情報について警告を受けました。このグループは、Equation Groupからの開示を受けていると主張しています。公開された資料には、複数のベンダーのファイアウォール製品の不正利用が含まれています。記事には、レガシーCisco PIXファイアウォールを悪用するために使用される可能性のあるBENIGNSUREの不正利用に関する情報が含まれています。

Shadow Brokersの情報開示に基づき、シスコはBENIGNSUREに類似した脆弱性の影響を受ける可能性がある他の製品の調査を開始しました。

Cisco Product Security Incident Response Team(PSIRT)は、該当プラットフォームを実行している一部のシスコのお客様が脆弱性を悪用していることを認識しています。

出典

この脆弱性の不正利用は、Cisco PIXのShadow Brokersグループによって公開されました。

Shadow Brokersの情報開示に基づき、シスコはBENIGNSUREに類似した脆弱性の影響を受ける可能性がある他の製品の調査を開始しました。

Cisco IOS、Cisco IOS XE、およびCisco IOS XRの脆弱性は、シスコ社内のセキュリティテストチームによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160916-ikev1

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.3	「該当製品」セクションと「脆弱性のある製品」セクションを更新。	該当製品および脆弱性のある製品	Interim	2016年10月5日
1.2	「該当製品」セクションを更新。	該当製品	Interim	2016年9月20日
1.1	「該当製品」セクションを更新。	該当製品	Interim	2016年9月19日
1.0	初回公開リリース	—	Interim	2016年9月16日

利用規約

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。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。