Cisco IOSソフトウェア Internet Key Exchange（IKE） メモリリーク の 脆弱性

High

アドバイザリーID : cisco-sa-20130925-ike

初公開日 : 2013-09-25 16:00

バージョン 1.0 : Final

CVSSスコア : 7.8

回避策 : Yes

Cisco バグ ID : CSCtx66011

CVE-2013-5473

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（IKE）プロトコルの脆弱性はリモート攻撃者非認証によりデバイスのリロードの原因となる可能性があるメモリリークを引き起こすようにする可能性があります。

脆弱性は影響を受けたソフトウェアによって不正 な IKE パケットの不正確な処理が原因です。攻撃者は IKE バージョン 1（IKEv1）を活用 する 機能で設定されたデバイスへ巧妙に細工された IKE 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。

IKEv1 または IKE バージョン 2（IKEv2）が設定されるとき IKEv1 が Cisco IOSソフトウェアおよび Cisco IOS XE ソフトウェアで自動的に有効に なるが、脆弱性は不正 な 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。

特定の条件では、正常な IKEv1 パケットによりまた Cisco IOSソフトウェアの該当するリリースはメモリをリークさせます場合があります。

IKEv1 だけこの脆弱性から影響を受けます。

エクスプロイトにより Cisco IOSソフトウェアはメモリリークを引き起こす割り当てられたメモリによりリリースします可能性があります。 支えられた攻撃はデバイスのリロードという結果に終るかもしれません。

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。この脆弱性を軽減する回避策がありません。

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-20130925-ike
注： 2013 年 9月 25 日、Cisco IOSソフトウェア Security Advisory によって組み込まれる書は 8 Cisco Security Advisory が含まれています。 すべてのアドバイザリは Cisco IOSソフトウェアの脆弱性に対処します。 各 Cisco IOSソフトウェア Security Advisory は正しい 2013 年 9 月のすべての Cisco IOSソフトウェア脆弱性はパブリケーションを組み込んだことアドバイザリ、また Cisco IOS ソフトウェア リリースで詳述される脆弱性を解決する Cisco IOS ソフトウェア リリースをリストします。

"Cisco Event Response: 半年ごと Cisco IOSソフトウェア Security Advisory は次のリンクのパブリケーションを」組み込みました:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep13.html

該当製品

修正済みソフトウェア

IKEv1 パケットだけこの脆弱性を引き起こす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。

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。

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)
- グループ ドメイン オブ インタープリテーション (GDOI)

デバイスが IKE 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。 デバイスが UDP ポート 500、UDP ポート 4500、または開いた UDP ポート 848 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 IPバージョン 4 (IPv4) または IP バージョン 6(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#
```

Cisco 製品で稼働している Cisco IOS ソフトウェア リリースを確認するには、機器にログインし show version コマンドを実行してシステムバナーを表示させます。 "Internetwork Operating System Software"、"Cisco IOS Software" あるいはこれらに類似するシステム バナーによってデバイスで Cisco IOS ソフトウェアが稼働していることを確認できます。 その後ろにイメージ名が括弧の間に表示され、続いて "Version" と Cisco IOS ソフトウエア リリース名が表示されます。 他の Cisco 機器では、 show version コマンドがない場合や、表示が異なる場合があります。

次の例は C3900-UNIVERSALK9-M のインストール済みイメージ名前と Cisco IOS ソフトウェア リリース 15.0(1)M1 を実行している Cisco製品を指定したものです:

```
Router> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_teamRouter> show version
Cisco IOS Software, C3900 Software (C3900-UNIVERSALK9-M), Version 15.0(1)M1, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Wed 02-Dec-09 17:17 by prod_rel_team
```

Cisco IOS ソフトウエアのリリース命名規則の追加情報は以下のリンクの "White Paper: http://www.cisco.com/web/about/security/intelligence/ios-ref.html の Cisco IOS および NX-OS ソフトウェア レファレンスガイド」。

脆弱性を含んでいないことが確認された製品

Cisco IOS XR ソフトウェアはこの脆弱性から影響を受けません。

Cisco ASA 5500 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。

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。

改訂履歴

リビジョン 1.0	2013-September-25	初版リリース

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。