

Cisco ASAソフトウェアのVPN ISAKMPにおけるDoS脆弱性

High

アドバイザリーID : cisco-sa-20151021-asa-ike

[CVE-2015-6327](#)

初公開日 : 2015-10-21 16:00

最終更新日 : 2015-11-12 14:15

バージョン 1.1 : Final

CVSSスコア : [7.8](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCus94026](#)

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適応型セキュリティアプライアンス(ASA)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1(v1)コードの脆弱性により、認証されていないリモートの攻撃者が該当システムのリロードを引き起こす可能性があります。

この脆弱性は、Internet Security Association and Key Management Protocol(ISAKMP)パケットの不適切な処理に起因します。攻撃者は、巧妙に細工されたUDPパケットを該当システムに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。不正利用に成功すると、攻撃者は該当システムのリロードを引き起こす可能性があります。

注：この脆弱性の不正利用に使用できるのは、該当システム宛てのトラフィックだけです。この脆弱性は、シングルコンテキストモードまたはマルチコンテキストモードで、ルーテッドファイアウォールモードに設定されたシステムにのみ影響します。また、この脆弱性は、IPv4 トラフィックと IPv6 トラフィックでトリガーされる可能性があります。

この脆弱性は、Cisco Bug ID [CSCus94026](#)([登録](#)ユーザ専用)として文書化され、Common Vulnerabilities and Exposures(CVE)IDとしてCVE-2015-6327が割り当てられています。

シスコ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しています。この脆弱性を軽減する回避策はありません。このアドバイザリーは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151021-asa-ike>

該当製品

次の製品で実行されているCisco ASAソフトウェアは、この脆弱性の影響を受けます。

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco ASA 5500-X シリーズ次世代ファイアウォール
- Cisco Catalyst 6500シリーズスイッチおよびCisco 7600シリーズルータ用Cisco ASAサービスモジュール
- Cisco ASA 1000V クラウド ファイアウォール
- Cisco 適応型セキュリティ仮想アプライアンス (ASA-v)

影響を受けるリリースの詳細については、このセキュリティアドバイザリの「修正済みソフトウェア」セクションを参照してください。

脆弱性のある製品

Cisco ASAソフトウェアは、システムがIKEv1 VPN接続を終了するように設定されている場合、この脆弱性の影響を受けます。

これには次の接続が含まれます。

- IKEv1を使用したLAN-to-LAN
- IPSec VPNクライアントを使用したリモートアクセスVPN
- Layer 2 Tunneling Protocol(L2TP)-over-IPSec VPN接続

次のVPN接続を終端するようにシステムが設定されている場合、Cisco ASAソフトウェアはこの脆弱性の影響を受けません。

- クライアントレス SSL
- AnyConnect SSL
- IKEv2 AnyConnect
- IKEv2 LAN-to-LAN

Cisco ASAがIKEv1 VPN接続を終端するように設定されているかどうかを確認するには、少なくとも1つのインターフェイスにクリプトマップを設定する必要があります。管理者は **show running-config crypto map | include interface** コマンドを使用して、出力が返されることを確認します。次の例は、 *outside* インターフェイスに設定された *cmap* という名前の暗号マップを示しています。

```
ciscoasa# show running-config crypto map | include interface  
crypto map outside_map interface outside
```

さらに、そのインターフェイスでIKEv1も有効にする必要があります。これは、 **show running-config crypto ikev1** コマンドまたは **show running-config | include crypto isakmp enable** コマンドを使用して、8.4より前のCisco ASAソフトウェアリリースに対応し、ikev1がインターフェイスで有効になっていることを確認します。

次の例は、Outsideインターフェイスで有効になっているIKEv1を示しています。

```
ciscoasa# show running-config crypto ikev1
crypto ikev1 enable outside
```

注：IKEv1はデフォルトでは設定されていません。

実行中のソフトウェアバージョンの確認脆弱性のあるバージョンのCisco ASAソフトウェアがアプライアンスで実行されているかどうかを確認するには、show versionコマンドを使用します。次の例は、Cisco ASAソフトウェアバージョン9.2(1)を実行しているアプライアンスの結果を示しています。

```
ciscoasa# show version | include Version
Cisco Adaptive Security Appliance Software Version 9.2(1)
Device Manager Version 7.4(1)
```

Cisco Adaptive Security Device Manager(ASDM)を使用してデバイスを管理しているお客様は、ログインウィンドウまたはCisco ASDMウィンドウの左上隅に表示される表でソフトウェアバージョンを確認できます。

脆弱性を含んでいないことが確認された製品

Cisco FirePOWER 9300 ASAセキュリティモジュールはこの脆弱性の影響を受けません

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。

セキュリティ侵害の痕跡

スレッド名 *IKE Daemon*でリロードするCisco ASAデバイスは、この脆弱性の不正利用を示す可能性があります。

スレッド名は、*crashinfo*ファイルの先頭にリストされます。*crashinfo*ファイルには、**show crashinfo**コマンドを使用してアクセスできます。次の例は、スレッド名 *IKE Daemon*の*crashinfo*ファイルを示しています。

```
ciscoasa# show crashinfo
: Saved_Crash
```

```
Thread Name: IKE Daemon
```

```
.
.
.
```

この脆弱性のアクティブなエクスプロイトが疑われる場合は、サポート組織に連絡して、クラッシュがこの脆弱性によるものかどうかを確認するためにトレースバックをデコードする必要があります。

回避策

この脆弱性を軽減する回避策はありません。ただし、管理者は影響を受ける機能を無効にすることができます。

修正済みソフトウェア

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。

次の表では、左の列に、Cisco ASA ソフトウェアのメジャー リリースを示します。中央の列が示すのは、本アドバイザリに記載された脆弱性によるメジャー リリースへの影響の有無、また、本脆弱性に対する修正を含む最初のマイナー リリースです。右の列は、メジャーリリースが次のアドバイザリに記載されているすべての脆弱性の影響を受けるかどうかと、これらの脆弱性の修正を含むリリースを示しています。

- [cisco-sa-20151021-asa-dhcp1](#)
- [cisco-sa-20150115-asa-dhcp](#)
- [cisco-sa-20151021-asa-dns1](#)
- [cisco-sa-20151021-asa-dns2](#)
- [cisco-sa-20151021-asa-ike](#)

次の表に示すように、適切なリリースにアップグレードする必要があります。

Cisco ASA メジャー リリース	この脆弱性に対する最初の修正リリース	2015年10月のASAセキュリティアドバイザリ
7.2	該当。8.2(5.58)以降に移行してください。	該当。8.2(5.58)以降に移行してください。
8.2	8.2 (5.58)	8.2 (5.58) 以降
8.3	該当。8.4(7.29)以降に移行してください。	該当。8.4(7.29)以降に移行してください。
8.4	8.4 (7.29)	8.4 (7.29)
8.5	該当。9.0(4.37)以降に移行してください。	該当。9.0(4.37)以降に移行してください。
8.6	該当。9.0(4.37)以降に移行してください。	該当。9.0(4.37)以降に移行してください。

8.7	8.7 (1.17)	8.7 (1.17) 以降
9.0	9.0 (4.37)	9.0 (4.37) 以降
9.1	9.1 (6.8)	9.1 (6.8) 以降
9.2	9.2(4)	9.2(4) 以降
9.3	9.3(3)	9.3 (3.6) 以降
9.4	Not affected	9.4(2) 以降
9.5	Not affected	Not affected

ソフトウェアのダウンロード

Cisco ASAソフトウェアは、Cisco.comのSoftware Centerから

<http://www.cisco.com/cisco/software/navigator.html>にアクセスしてダウンロードできます。

Cisco ASA 5500シリーズ適応型セキュリティアプライアンスおよびCisco ASA 5500-X Next Generation Firewallの場合は、次のパスに移動します。暫定バージョンを検索するには、ダウンロードページの左側にある[All Releases] > [Interim] をクリックします。

[製品(Products)] > [セキュリティ(Security)] > [ファイアウォール(Firewalls)] > [適応型セキュリティアプライアンス(ASA)(Adaptive Security Appliances (ASA))] > [ASA 5500シリーズ適応型セキュリティアプライアンス(ASA)] > <Cisco ASAモデル> > [適応型セキュリティアプライアンス(ASA)ソフトウェア(Adaptive Security Appliance (ASA) Software)] Cisco Catalyst 6500シリーズスイッチおよびCisco 7600シリーズルータ用Cisco ASAサービスモジュールの場合は、次のパスに移動します。暫定バージョンを検索するには、ダウンロードページの左側にある[All Releases] > [Interim] をクリックします。

[製品(Products)] > [Cisco Interfaces and Modules] > [Services Modules] > [Catalyst 6500 Series / 7600 Series ASA Services Module] > [Adaptive Security Appliance(ASA)Software] Cisco ASA 1000Vクラウドファイアウォールの場合は、次のパスに移動します。

[製品(Products)] > [セキュリティ(Security)] > [ファイアウォール(Firewalls)] > [適応型セキュリティアプライアンス(ASA)(Adaptive Security Appliances (ASA))] > [ASA 1000Vクラウドファイアウォール(ASA 1000V Cloud Firewall)] Cisco適応型セキュリティ仮想アプライアンス(ASAv)の場合は、次のパスに移動します。

[製品(Products)] > [セキュリティ(Security)] > [ファイアウォール(Firewalls)] > [適応型セキュリティアプライアンス(ASA)(Adaptive Security Appliances (ASA))] > [適応型セキュリティアプライアンス(ASA)(Adaptive Security Appliance (ASA) Software)] Cisco FirePOWER 9300 ASAモジュールの場合は、次のパスに移動します。

[製品(Products)] > [セキュリティ(Security)] > [ファイアウォール(Firewalls)] > [適応型セキュリティアプライアンス(ASA)(Adaptive Security Appliances (ASA))] > [Firepower 9000シリーズ(Firepower 9000 Series)] > [Firepower 9300セキュリティアプライアンス(Firepower 9300 Security

Appliance)] > [適応型セキュリティアプライアンス(ASA)ソフトウェア(Adaptive Security Appliance (ASA) Software)]

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) は、本アドバイザリに記載されている脆弱性の不正利用事例やその公表を確認していません。

出典

この脆弱性は内部セキュリティテストで発見されました。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151021-asa-ike>

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	Cisco ASA 9.3トレインの推奨リリースバージョンを修正。	修正済みソフトウェア	Final	2015年11月12日
1.0	初回公開リリース	-	Final	2015年10月21日

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、単独の転載や意識を施した場合、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。

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。