

Cisco Intrusion Prevention Systemのキー再生成におけるHTTPSのDoS脆弱性

Medium	アドバイザーID : Cisco-SA-	CVE-
	20150220-CVE-2015-0631	2015-
	初公開日 : 2015-02-20 20:22	0631
	バージョン 1.0 : Final	
	CVSSスコア : 5.4	
	回避策 : No Workarounds available	
	Cisco バグ ID : CSCui25688	

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 Intrusion Prevention System(IPS)ソフトウェアのWeb管理インターフェイスで使用されるSSL/TLSサブシステムの脆弱性により、認証されていないリモートの攻撃者がサービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、7.2より前のイメージからイメージ7.2以降にアップグレードする際に、該当デバイスの暗号証明書とキーを再生成する際に発生する可能性のある競合状態に起因します。攻撃者は、キー再生成の処理中に管理インターフェイスとの多数のHTTPS接続をネゴシエートすることで、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、攻撃者はDoS状態を作成できる可能性があります。この状態は、デバイスが再起動されるまで続きます。

この脆弱性は、Webサーバに関連付けられた管理インターフェイスのTCPポートとIPアドレスに宛てられたSSL/TLSトラフィックによってのみ引き起こされます。デフォルトのTCPポートは443です。センシングインターフェイスを介して該当デバイスを通過するパケットは、この脆弱性のトリガーには使用できません。

シスコは、セキュリティ通知で脆弱性を確認し、ソフトウェアアップデートをリリースしました。

シスコはCVSSスコアを通じて、機能不正利用コードが存在することを示していますが、このコードが一般に公開されているかどうかは不明です。

該当製品

影響を受ける製品バージョンの完全なリストについては、Cisco Bug ID [CSCui25688](#)を参照してください。

脆弱性のある製品

このアラートが最初に公開された時点では、Cisco IPSバージョン7.2(1)E4には脆弱性が存在していました。Cisco IPSの新しいバージョンにも脆弱性が存在する可能性があります。

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

適切なアップデートを適用することを推奨します。

信頼できるユーザだけにネットワークアクセスを許可することを推奨します。

IPベースのアクセスコントロールリスト(ACL)を使用して、信頼できるシステムだけに該当システムへのアクセスを許可することを検討することもできます。

管理者は、堅実なファイアウォール戦略を使用して、影響を受けるシステムを外部からの攻撃から保護できます。

影響を受けるシステムを監視することを推奨します。

修正済みソフトウェア

有効な契約を結んでいるシスコのお客様は、シスコのサポートチームに連絡して、この脆弱性の修正を含むソフトウェアバージョンへのアップグレードをサポートしてもらう必要があります。契約を結んでいないお客様は、Cisco Technical Assistance Center(TAC)に1-800-553-2447または1-408-526-7209で連絡するか、tac@cisco.comで電子メールを介してサポートを受けることができます。

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。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20150220-CVE-2015-0631>

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初版リリース	適用外	Final	2015年2月20日

利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザー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。