OpenSSL RSAの一時キー暗号化ダウングレードの脆弱性

Mediu
m

アドバイザリーID : Cisco-SA-20150113-CVE-2015-0204 CVE-2015-0204

初公開日 : 2015-01-13 19:57

最終更新日 : 2015-09-25 12:45

バージョン 14.0 : Final

CVSSスコア : 5.0

回避策 : No Workarounds available

Cisco バグ ID : CSCus43003 CSCus42791 CSCus43000 CSCus42792 CSCus42753 CSCus42710 CSCus42754 CSCus42831 CSCus42952 CSCus42996 CSCus42751 CSCus42752 CSCus42713 CSCus42834 CSCus42758 CSCus42879 CSCus42711 CSCus42755 CSCus42712 CSCus42833 CSCus42954 CSCus42836 CSCus42958 CSCus77211 CSCus42917 CSCut14256 CSCus43052 CSCus42721 CSCus42883 CSCus43015 CSCus42763 CSCus42840 CSCus43016 CSCus42724 CSCus42768 CSCus42801 CSCus42966 CSCus42967 CSCut82321 CSCus42766 CSCus42723 CSCus42800 CSCus42726 CSCus42968 CSCus42727 CSCus42804 CSCus43020 CSCus42772 CSCus43022 CSCus42775 CSCus42699 CSCus42732 CSCus42853 CSCus42850 CSCus44478 CSCus42851 CSCus42972 CSCus42812 CSCus42739 CSCus42816 CSCus42737 CSCus42814 CSCus42738 CSCus42818 CSCus61884 CSCus60116 CSCum57065 CSCus42781 CSCus42742 CSCus42786 CSCus42787 CSCus42982 CSCus42785 CSCus42983 CSCus42702 CSCus42900 CSCus42901 CSCus42821 CSCus42701 CSCus42706 CSCus42827 CSCus42904 CSCus42828 CSCus42748 CSCus42705 CSCus42749 CSCus42908 CSCus42829 CSCus42906 CSCus42709 CSCus43041

容の齟齬がある場合には、英語原文が優先します。

概要

OpenSSLの脆弱性により、認証されていないリモートの攻撃者がセキュリティ制限をバイパスできる可能性があります。

この脆弱性は、RSA一時キーの不適切な処理に起因します。ネットワークの特権を持つ攻撃者は、脆弱なOpenSSLライブラリを使用するアプリケーションを使用して脆弱な一時RSAキーをシステムに返すことで、この脆弱性を不正利用する可能性があります。安全でない一時キーが処理されると、暗号化による保護が減少し、攻撃者がセキュリティ保護をバイパスできる可能性があります。

OpenSSLが脆弱性を確認し、ソフトウェアアップデートをリリースしました。

この脆弱性をエクスプロイトするには、攻撃者がターゲットシステムに一時的なRSAキーを返すために、信頼されたネットワークまたは内部ネットワークへの特権ネットワークアクセスを必要とする可能性があります。このアクセス要件により、不正利用が成功する可能性が大幅に制限されます。

該当製品

OpenSSLは次のリンクでセキュリティアドバイザリをリリースしました :CVE-2015-0204

BlackBerryは、CVE-2015-0204のリンクでセキュリティアドバイザリをリリースしました。

FreeBSDは次のリンク先でVuXMLドキュメントを公開しています。 OpenSSL — multiple vulnerabilities

HPは、セキュリティ情報c04604357、c04635715、c0467933、c04765169、 c04762744、c04773241、c04765115、c04774021、およびc04805275(HPSBGN03299 SSRT101987、HPSBOV03318、HPSBUX03334 SSRT10200000、をでリリースしています。 HPSBMU03397 SSRT102192、 HPSBMU03394 SSRT102187、HPSBMU03345 SSRT102095、HPSBMU03413、HPSBMU03396、およびHPSBMU03422 SSRT101438

IBMは次のリンクでセキュリティアドバイザリをリリースしました：CVE-2015-0204

Red Hatは、バグ1180184に関する公式のCVEステートメントとセキュリティアドバイザリを次のリンクでリリースしました：CVE-2015-0204、RHSA-2015:0066、およびRHSA-2015:0849

Splunkは次のリンクからセキュリティアドバイザリをリリースしました。SP-CAANZ7

脆弱性のある製品

次のOpenSSLバージョンには脆弱性が存在します。

- 1.0.1kより前のOpenSSLバージョン
- 1.0.0pより前のOpenSSLバージョン
- 0.9.8zdより前のOpenSSLバージョン

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。

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

OpenSSLは、次のリンクで更新されたソフトウェアをリリースしました。

OpenSSL 1.0.1の場合
OpenSSL 1.0.1k

OpenSSL 1.0.0の場合
OpenSSL 1.0.0p

OpenSSL 0.9.8の場合
OpenSSL 0.9.8zd

BlackBerryをご使用のお客様には、この脆弱性を軽減するために、ベンダーのアドバイザリに記載されている解決手順に従うことをお勧めします。

CentOSパッケージは、**up2date**または**yum**コマンドを使用して更新できます。

FreeBSDは次のリンクからports collection updatesをリリースしました： Ports Collection Index

HPは、セキュリティ情報の「解決策」セクションで説明されているように、お客様向けの更新されたソフトウェアをリリースしました。

HPは次のリンクで更新されたソフトウェアをリリースしています。
HP Version Control Agent(VCA)7.3.5
Windowsの場合 – X86
Windowsの場合 – X64
Linux用

HP Systems Insight Managerバージョン7.5.0

- x86用Linuxの場合
- MSウィンドウ

HP Version Control Repository Manager(VCRM)バージョン7.5.0

- Windows の場合
- Linux用

HP System Management Homepageバージョン7.2.6 for Windows 2003
IBMユーザは、このアドバイザリの「ソリューション」セクションに記載されている手順に従って、修正を適用することをお勧めします。

Red Hatは、 Red Hat Networkのリンクから、登録ユーザ向けの更新ソフトウェアをリリースしました。 Red Hatパッケージは、Red Hat Enterprise Linuxバージョン5以降でyumツールを使用して更新できます。

Splunk Enterpriseは、次のリンクで更新されたソフトウェアをリリースしています。

- Splunk Enterprise 6.2.3
- Splunk Light 6.2.3

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-20150113-CVE-2015-0204

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 . 0	HPは、OpenSSL RSAの一時キー暗号化ダウングレードの脆弱性に対処するために、追加のセキュリティ情報とソフトウェア更新プログラムをリリースしました。	適用外	Final	2015年8月2

				5日
12.0	HPは、OpenSSL RSAの一時キー暗号化ダウングレードの脆弱性に対処するために、追加のセキュリティ速報とソフトウェアアップデートをリリースしました。	適用外	Final	2015年8月21日
11.0	HPは、OpenSSL RSAの一時キー暗号化ダウングレードの脆弱性に対処するために、追加のセキュリティ速報とソフトウェアアップデートをリリースしました。	適用外	Final	2015年8月20日
10.0	HPは、OpenSSL RSAの一時キー暗号化ダウングレードの脆弱性に対処するために、追加のセキュリティ速報とソフトウェアアップデートをリリースしました。	適用外	Final	2015年5月21日
9.0	Splunkは、OpenSSL RSAの一時キー暗号化ダウングレードの脆弱性に対処するアドバイザリと更新されたソフトウェアをリリースしました。	適用外	Final	2015年5月6日
8.0	Red Hatは、OpenSSL RSA一時キー暗号化ダウングレードの脆弱性に対処するための追加のセキュリティアドバイザリと更新パッケージをリリースしました。	適用外	Final	2015年4月17日

7.0	CentOSは、OpenSSL RSAの一時キー暗号化ダウングレードの脆弱性に対処するための追加の更新パッケージをリリースしました。	適用外	Final	2015年4月15日
6.0	HPは、OpenSSL RSAの一時キー暗号化ダウングレードの脆弱性に対処するために、追加のセキュリティ速報と更新されたソフトウェアをリリースしました。	適用外	Final	2015年4月14日
5.0	BlackBerryは、OpenSSL RSA一時キー暗号化ダウングレードの脆弱性に対処するためのセキュリティアドバイザリと更新されたソフトウェアをリリースしました。	適用外	Final	2015年4月3日
4.0	HPは、OpenSSL RSAの一時キー暗号化ダウングレードの脆弱性に対処するためのセキュリティ速報と更新されたソフトウェアをリリースしました。	適用外	Final	2015年3月30日
3.0	IBMは、OpenSSL RSA一時キー暗号化ダウングレードの脆弱性に対処するためのセキュリティアドバイザリと修正をリリースしました。	適用外	Final	2015年2月6日
2.0	Red Hatは、OpenSSL RSAの一時キー暗号化ダウングレードの脆弱性に対処するためのセキュリティアドバイザリと更新パッケージをリリースしました。CentOSは、この脆弱性	適用外	Fina	2015

	に対処するための更新されたパッケージもリリースしています。		I	年1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。

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。