一般社団法人電子情報技術産業協会
一般社団法人コンピュータソフトウェア協会
一般社団法人情報サービス産業協会
一般社団法人日本情報システム・ユーザー協会
特定非営利活動法人日本ネットワークセキュリティ協会 御中

OpenSSL の脆弱性対策の実施徹底について（協力依頼）

平成２６年４月１８日
経　済　産　業　省
商 務 情 報 政 策 局
情 報 処 理 振 興 課
情 報 通 信 機 器 課
情報セキュリティ政策室

すでに報道や各機関からの注意喚起等のアナウンスにてご存知かと思われますが、Web サイトなどで通信内容を暗号化するために使われているソフトウェアのひとつである「OpenSSL」に情報漏えいの脆弱性が発見されました。独立行政法人情報処理推進機構（IPA）及び一般社団法人 JPCERT/CC より 4 月 8 日から断続的に注意喚起をさせていただいております。本脆弱性を悪用した攻撃がすでに観測されており、会員企業各社への周知徹底等、ご協力をお願いいたします。

・IPA 発表: OpenSSL の脆弱性対策について(CVE-2014-0160)
https://www.ipa.go.jp/security/ciadr/vul/20140408-openssl.html
・JPCERT/CC 発表: OpenSSL の脆弱性に関する注意喚起
https://www.jpcert.or.jp/at/2014/at140013.html

【対象バージョンと影響について】
この OpenSSL は会員登録機能を持つ Web サイトや通販サイト、インターネットバンキングなどあらゆる Web サービスにおいて世界中で使用されており、今回発見された脆弱性を悪用された場合、利用者が入力した個人情報やクレジットカード情報などを悪意ある第三者に窃取される恐れがあります。
本脆弱性を悪用する攻撃方法がインターネット上ですでに公開されてしまっており、警察庁の発表によるとこの攻撃と見られる通信が観測されているとのことで至急の対策が必要です。また、この脆弱性を悪用した攻撃が行われた場合、攻撃の痕跡が運用されているシステムの通信記録上に残らないため、攻撃を検知すらできない可能性があるとともに、

すでに攻撃を受けてしまっている懸念があります。

対象となるのは以下のバージョンとなります。

・OpenSSL 1.0.1 から 1.0.1f

・OpenSSL 1.0.2-beta から 1.0.2-beta1

また、OpenSSL が組み込まれている製品やソフトウエアも本脆弱性の影響を受ける可能性がありますので、製品やソフトウエアの開発元の情報をご確認ください。

【社内等における対策指示の徹底】

すでに IPA などからの注意喚起を元に、多くの企業等が本脆弱性への対処に取り組まれているかと思われますが、未だ未対応の Web サイトがある旨報道されているところ、残る各社における対策実施を速やかに行う必要があります。つきましては、技術的に必要な対策を下記の通り周知させていただきますので、団体各社において担当部門への対策実施指示が徹底され、自社システムのみならず、他社への提供サービスにおいても対策が速やかに実施されるよう、各社への情報展開等ご協力をお願いいたします。

記

１．脆弱性の解消するためのアップデート作業

本脆弱性を修正したバージョンへの速やかなアップデート等を実施してください。

○The OpenSSL Project が提供する OpenSSL を直接利用している場合は、十分なテストを実施の上対象サーバの OpenSSL を 1.0.1g 以降にアップデートしてください。

・修正済みバージョン：OpenSSL 1.0.1g

・ダウンロード元： http://www.openssl.org/source/

なお、OpenSSL 1.0.2-beta については、2014 年 4 月 8 日現在、修正済みのバージョンは公開されていません。対応方法は下記手順にてご対応ください。

○The OpenSSL Project が提供する OpenSSL を直接利用している場合で、かつ、アップデートが難しい場合には、-DOPENSSL_NO_HEARTBEATS オプションを有効にして OpenSSL を再コンパイルしてください。

○上記以外の形態で OpenSSL を利用している場合、および、OpenSSL を組み込んだ製品を利用している場合は、提供元に対策を確認してください。

２．サーバ証明書の再設定

ウェブサイトで OpenSSL を利用している場合、秘密鍵が既に漏えいしている可能性があります。ウェブサイト運営者は脆弱性の解消後、これまで利用していた証明書を失効させ、新しい秘密鍵を用いて証明書を再取得・再設定してください。証明書の失効・再発

行等の手続きは、各認証局へ確認ください。

〇認証局に対して、証明書の失効と再発行を依頼してください。再発行依頼の際には、これまで使っていた秘密鍵を破棄し、新しく生成した秘密鍵を用いてください。

〇認証局から再発行された証明書を、対象サーバに設定してください。

３．ウェブサイト利用者へのアナウンス

https でアクセスできるウェブサイトを運営している場合、ウェブサイト運営者は状況に応じて、利用者へ以下をアナウンスするよう検討してください。本脆弱性のアナウンスになりすました不正なメールが配信される恐れがありますので、利用者へのメール配信だけを実施せず、ウェブサイトでのアナウンスをあわせて実施するようお願いいたします。

・当該脆弱性の影響を受けないことを確認したウェブサイト運営者は、影響を受けないことを利用者アナウンスしてください。

・対策を完了したウェブサイト運営者は、対策を完了したことを利用者アナウンスしてください。その際、利用者へのお願いがあれば併記してください（たとえばパスワードの変更など)。

４．その他参考情報

各企業においては、自組織で Web サーバを管理している場合とクラウドサービスや他企業へのアウトソーシングをされている場合があるかと思われます。それぞれの場合において、「自社サイトが当該脆弱性を有しているのか」確認するために下記方法を参考情報として記載いたします。

1) 自社管理している場合

OpenSSL のバージョンに関しては、コマンド設定で確認して下さい

2) 他社サービスを活用している場合（クラウド、アウトソース等）

OpenSSL コマンドで確認するのができないケースでは､サービス提供事業者に確認するか、あるいは、早急の確認には、OpenSSL のセキュリティ上の問題(脆弱性)をチェックするサービスやツールを使用することで、自組織が影響を受けるかどうかを確認できます。ご参考までに、サービスやツールの一部をお知らせいたします。ただし、各種サービスやツールの安全性やチェック結果を担保することはできないため、各組織が信用できるものを自己責任で使用いただくことになります。また、当該ツールについては必ず自組織向けに使用するよう注意をしてください。

＜サービス例＞

・Heartbleed 脆弱性検査

http://ssl.white.hacker.jp/hb/hb

・設定状況や信頼性がわかる！SSL チェックツール｜GMO グローバルサイン

https://sslcheck.globalsign.com/ja

・Qualys SSL Labs - Projects / SSL Server Test

https://www.ssllabs.com/ssltest/index.html

また、IPA においては下記一般のウェブサイト利用者向けの情報提供ページを用意しておりますで、あわせてご参考ください。

・OpenSSL の脆弱性に対する、ウェブサイト利用者（一般ユーザ）の対応について

http://www.ipa.go.jp/security/ciadr/vul/20140416-openssl_webuser.html

上記脆弱性の技術的対策に関する問合せ先

一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）
MAIL: info@jpcert.or.jp
TEL:03-3518-4600　　FAX: 03-3518-4602

または

IPA　技術本部　セキュリティセンター

E-mail：vuln-inq@ipa.go.jp

※本文書の取扱いについて

なお、本文書については、自組織以外を含む必要な範囲への情報転送が可能です。ただし、Web サイトや公開のメーリングリストなどを使用して本文書全文をそのまま一般へ公開することは避け、必要な箇所を適宜編集した上で展開いただくようお願いいたします。
特に、上記連絡先のメールアドレス等をそのまま Web サイトにテキスト文として記載しないようご注意ください。