

「OpenSSL」の古いバージョンを利用しているウェブサイトへの注意喚起

ーウェブサイト運営者は脆弱性対策情報を収集し、バージョンアップを！ー

IPA（独立行政法人情報処理推進機構、理事長：西垣 浩司）は、オープンソースの「OpenSSL」（開発者：OpenSSL Project）の脆弱性について、「既に脆弱性対策を施したバージョンが公表されているにも関わらず、未適用のウェブサイトがある」旨の届出が増加していることから、本ソフトウェアを利用しているウェブサイト運営者に対し、迅速なバージョンアップ実施を呼びかけるため、「注意喚起」を発することとしました。

2008年11月頃から、OpenSSL（SSL/TLS実装¹）を使用している複数のウェブサイトに対して、「開発者から脆弱性対策を実施したバージョンが既に公表されているのにも拘らず、ウェブサイト運営者はそのバージョンを適用していないのではないか？」という旨の届出が増加しています。

具体的には、2005年10月に公表された「OpenSSLにおけるバージョン・ロールバックの脆弱性²」の修正バージョン未適用の届出が、2009年8月末までに88件ありました。ウェブサイト運営主体の内訳は、民間企業が50、地方公共団体が27、政府機関が9、団体（協会・組合など）が2となっています（図1）。

IPAでまとめた「2008年のコンピュータ不正アクセス届出状況³」では、実被害があった原因の第1位は「IDやパスワードの管理・設定の不備」で35件（29%）、第2位が「古いバージョンの使用やパッチの未適用」で16件あり、13%を占めています。近年、脆弱性の公表から、その脆弱性を狙った攻撃が発生するまでの間隔が短くなっています。ウェブサイト運営者は、自組織が使用しているソフトウェアの脆弱性対策情報を定期的に収集し、未対策の場合はソフトウェアに修正プログラム（パッチ）を適用する、もしくはソフトウェアをバージョンアップする必要があります。

なお、脆弱性関連情報の取扱いの効率化を図るため、2009年7月8日の「情報セキュリティ早期警戒パートナーシップガイドラインの改訂⁴」で、このようなウェブサイトの不適切な運用に関しては、注意喚起などの方法で広く対策実施を促した後に処理を取りやめることとなりました。今後、「OpenSSL」の古いバージョンの利用によるウェブサイトの脆弱性の届出は受理しますが、取扱いを終了し、統計情報として活用します。

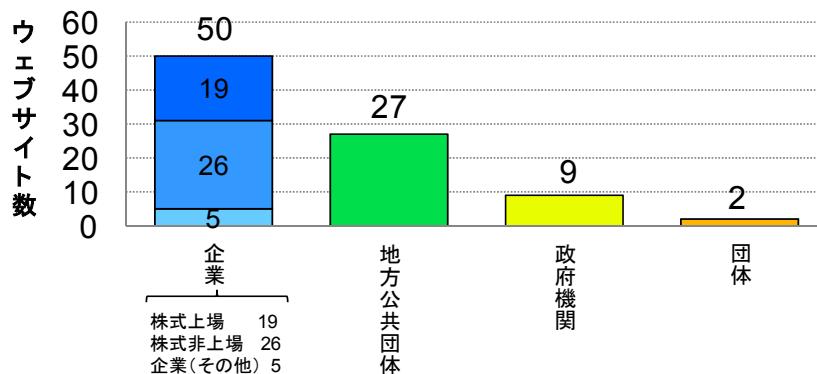


図1. OpenSSLバージョンアップ未実施のウェブサイトに対する届出の運営主体の内訳

¹ 暗号化通信の方式であるSSL: Secure Sockets Layer および TLS: Transport Layer Security を実現するための、ライブラリ等を含む一連のソフトウェア。

² 詳細は次の URL を参照下さい。http://jvndb.jvn.jp/jvndb/JVNDB-2005-000601

³ 詳細は次の URL を参照下さい。http://www.ipa.go.jp/security/txt/2009/documents/2008all-cra.pdf

⁴ 情報セキュリティ早期警戒パートナーシップガイドライン。http://www.ipa.go.jp/security/ciadr/partnership_guide.html

1. 「OpenSSL」の脆弱性について

OpenSSLには、2005年10月に公表されたバージョン・ロールバックの脆弱性があります。

この脆弱性を悪用されると、図2に示すように、弱い暗号化通信方式を強制されてしまいます。このため、暗号通信を解読され、情報が漏えいする可能性があります。

また、OpenSSLには、バージョン・ロールバックの脆弱性の他にも、バッファオーバーフローの脆弱性やサービス運用妨害 (DoS) の脆弱性が公表されています。

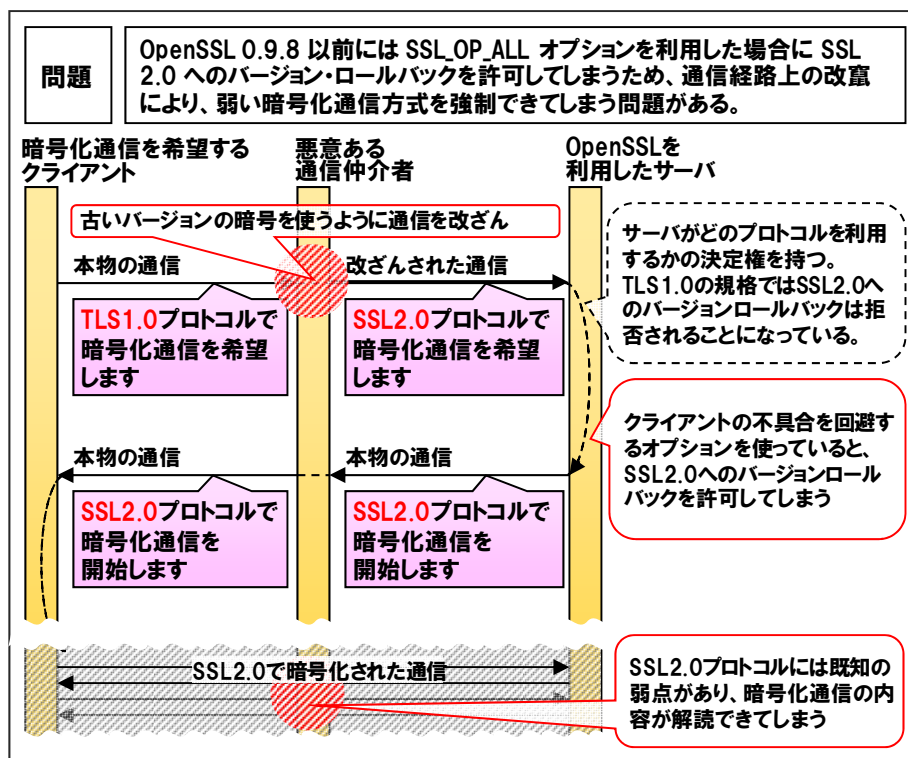


図 2. OpenSSL におけるバージョン・ロールバックの脆弱性

2. 対策

2.1 対策方法

「OpenSSL」を利用しているウェブサイト運営者は、脆弱性対策を施した最新版へのバージョンアップを実施してください。現時点で既知の脆弱性については2009年3月25日に公開されたOpenSSL 0.9.8k以降において対策が施されているため、これ以前のものを使用している場合は、OpenSSL 0.9.8k以降へのバージョンアップが必要です。

また、今後新たな脆弱性が公表される可能性がありますので、定期的に関係者の発信する情報を収集し、最新版へのバージョンアップを実施してください。

- ・ OpenSSL: News, Project Newsflash : <http://www.openssl.org/news/>

2.2 使用中の「OpenSSL」のバージョン確認方法

「OpenSSL」の管理者は下記の手順により、使用中の「OpenSSL」のバージョン確認が可能です。なお、パッケージから「OpenSSL」をインストールした場合は、バージョン表記が異なる可能性があるため注意が必要です。

- ・ コマンドラインから openssl コマンドを実行する (図 3)

```
$ openssl version
OpenSSL 0.9.8k 25 Mar 2009
```

図 3. OpenSSL のバージョン確認例

3.脆弱性対策情報の収集方法

3.1 脆弱性対策情報データベース JVN iPedia の活用

JVN iPedia(<http://jvndb.jvn.jp/>)は、日本国内で使用されているソフトウェア製品の脆弱性対策情報を収集するためのデータベースを目指し、(1) 国内のソフトウェア製品開発者が公開した脆弱性対策情報、(2) 脆弱性対策情報ポータルサイト JVN⁵で公表した脆弱性対策情報、(3) 米国立標準技術研究所 NIST⁶の脆弱性データベース「NVD⁷」が公開した脆弱性対策情報の中から情報を収集、翻訳し、2007年4月25日から公開しており、2009年9月現在、7,200件を超える情報を格納しています。

JVN iPedia では開発者ごとに公開されている脆弱性対策情報を一か所に集約することで、複数の開発者から情報を収集する手間を省き、効率的な情報収集を可能としています。また、さまざまな組織が公開する情報を横断的に知りたい場合や、特定のソフトウェアに存在する脆弱性について知りたい場合も、図4に示すように、複数の検索条件を指定することにより、効率的に情報を収集することができます。

さらに、検索結果一覧の中から、概要や影響を受けた時の深刻度、影響を受けるシステム、対策情報などの詳細な脆弱性対策情報が入手できます。

脆弱性対策情報データベース検索

検索キーワード: 検索

検索結果一覧

検索キーワード、ベンダ名、製品などを指定

発見日や更新日、深刻度も指定可能

脆弱性対策のための詳細情報

JVNDB-2005-000601 [English]
OpenSSL におけるバージョン・ロールバックの脆弱性

概要

OpenSSL Project より提供されている OpenSSL には、バージョン・ロールバックが可能な脆弱性が存在します。

TLS プロトコルを定めている RFC2246 では、バージョン・ロールバック攻撃を避けるために、TLS 1.0 が使用できる場合には SSL 2.0 を利用しないことを定めています。本脆弱性情報は、情報セキュリティ早期警戒パートナーシップに基づき下記の方が IP AI に報告し、JPCERT/CC がベンダおよびCERT/CC との調整を行いました。

報告者: 産業技術総合研究所 情報セキュリティ研究センター 大岩 寛 氏

問題

OpenSSL 0.9.8 以前には SSL_OP_ALL オプションを利用した場合に SSL 2.0 へのバージョン・ロールバックを許可してしまうため、通信経路上の改ざんにより、強い暗号化通信方式を強制できてしまう問題がある。

暗号化通信を希望するクライアント

古いバージョンの暗号を使うように通信を改ざん

必要ある通信仲介者

改ざんされた通信

OpenSSL を利用したサーバ

サーバなどのプロトコルを利用するかの決定権を持つ。TLS 1.0 の規格では SSL 2.0 へのバージョン・ロールバックは指責されることになっている。

本物の通信

TLS 1.0 プロトコルで暗号化通信を希望します

SSL 2.0 プロトコルで暗号化通信を希望します

クライアントの不具合を回避するオプションを使っていると、SSL 2.0 へのバージョン・ロールバックを許可してしまう

本物の通信

SSL 2.0 プロトコルで暗号化通信を開始します

SSL 2.0 プロトコルで暗号化通信を開始します

SSL 2.0 で暗号化された通信

SSL 2.0 プロトコルには既知の弱点があり、暗号化通信の内容が解読できてしまう

図4. JVN iPedia の脆弱性対策情報の検索機能

3.2 脆弱性対策情報収集ツール MyJVN の活用

MyJVN(<http://jvndb.jvn.jp/apis/myjvn/>)は、JVN iPedia に登録された多数の情報の中から、利用者が、利用者自身に関係する情報のみを効率的に収集できるように、フィルタリング条件設定機能、自動再検索機能、脆弱性対策チェックリスト機能などを有し、2008年10月23日から公開しています。

図5に示すように、利用者が収集したい製品開発者やソフトウェアなどのフィルタリング条件を一度設定しておけば、その後は MyJVN へアクセスするだけで、設定したソフトウェアの最新の情報だけが自動的に表示され、非常に効率的に情報を収集することができます。

更に、脆弱性対策が具体的にどこまでできているか確認するための、脆弱性対策チェックリストを出力する機能も有しています。

⁵ Japan Vulnerability Notes. 脆弱性対策情報ポータルサイト。製品開発者の脆弱性への対応状況を公開し、システムのセキュリティ対策を支援しています。IPA、JPCERT/CC が共同で運営しています。 <http://jvn.jp/>

⁶ National Institute of Standards and Technology. 米国国立標準技術研究所。米国の科学技術分野における計測と標準に関する研究を行う機関。 <http://www.nist.gov/>

⁷ National Vulnerability Database. NIST が運営する脆弱性データベース。 <http://nvd.nist.gov/home.cfm>

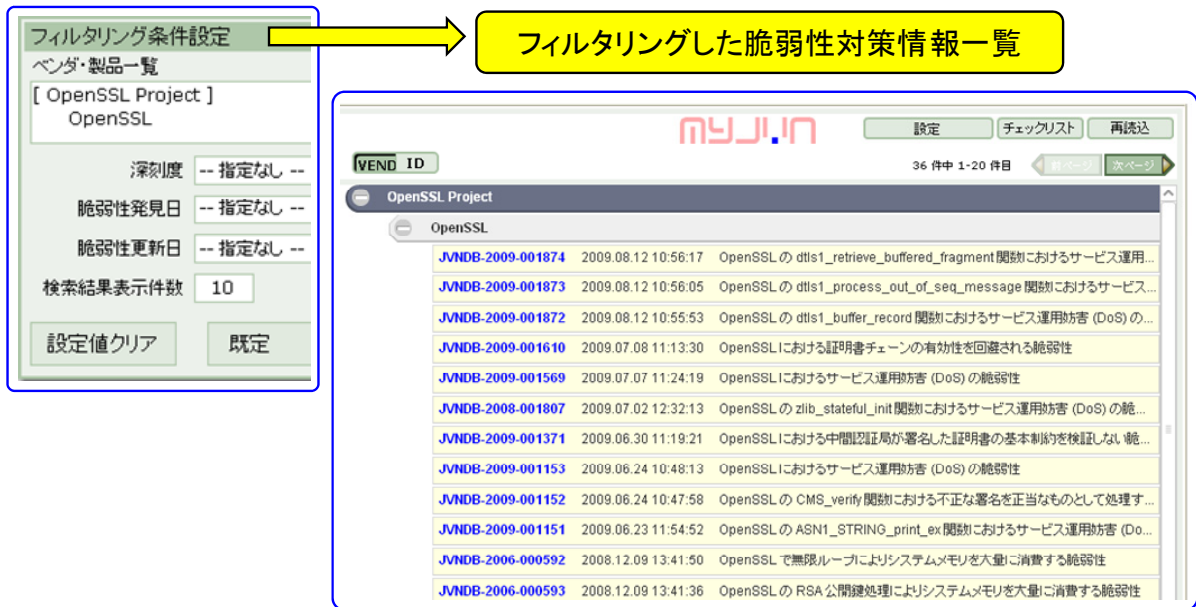


図 5. My JVN の脆弱性対策情報のフィルタリング機能

3.3 パッチ対策の緊急度の評価

IPA では、脆弱性の深刻度を評価した CVSS⁸基本値を公表しています。JVN iPedia の CVSS 計算ツール⁹ (図 6) を用いると、各組織での対象製品の利用範囲や、攻撃を受けた場合の被害の大きさなどを考慮し、製品利用者自身が脆弱性への対応を判断するための CVSS 環境値を計算することが可能です。

この結果を基に、例えば CVSS 環境値が 7.0 以上は緊急にパッチ、4.0 以上は月次パッチ、それ以外は定期保守でパッチなど、パッチ対策の緊急度の見極めに活用できます。



図 6. JVN iPedia の CVSS 計算ツール

- 本件に関するお問い合わせ先
IPA セキュリティセンター 山岸／渡辺
Tel: 03-5978-7527 Fax: 03-5978-7518 E-mail: vuln-inq@ipa.go.jp
- 報道関係からのお問い合わせ先
IPA 戦略企画部広報グループ 横山／大海
Tel: 03-5978-7503 Fax: 03-5978-7510 E-mail: pr-inq@ipa.go.jp

⁸ 共通脆弱性評価システム CVSS v2 概説。http://www.ipa.go.jp/security/vuln/SeverityCVSS2.html

⁹ http://jvn.db.jvn.jp/cvss/ScoreCalc2.swf?fn=parameter2.xml&lang=ja&g=1