第69回

IT エンジニア必須の 最新用語解説

TEXT：㈲オングス 杉山 貴章 SUGIYAMA Takaaki
takaaki@ongs.co.jp

テーマ募集
本連載では、最近気になる用語など、今後取り上げてほしいテーマを募集しています。sd@gihyo.co.jp 宛にお送りください。

OpenSSL とその派生プロジェクト

セキュリティ問題に揺れる「OpenSSL」

OpenSSLは、暗号通信のためのSSLおよびTLSプロトコルを実装したオープンソースソフトウェアです。さまざまなOSやプログラミング言語に対応しており、ソフトウェアに組み込むライブラリとして利用することができるため、幅広い分野で標準的に利用されています。

2014年に入って、このOpenSSLに2つの重大な脆弱性が報告されました。1つはTLSのHeartbeat拡張機能に混入した「Heartbleed」と呼ばれる脆弱性です。Heartbeat拡張とは、ネットワークリソース間で暗号通信のセッション保持時間を延ばすためのしくみで、OpenSSLでは2012年3月にリリースされた1.0.1よりサポートされました。しかしこの実装にメモリの取り扱いに関する深刻なバグがあり、不適切なリクエストを送ることで、本来は参照することができないサーバのメモリの内容を最大で64KBまで読み取ることができてしまうことが判明しました。それがHeartbleedです。この脆弱性を利用することで攻撃者は痕跡を残すことなくメモリの内容を読むことができ、場合によっては秘密鍵などの重大な機密情報が盗まれ、暗号化そのものが無力化する恐れもあります。

Heartbleedの熱が冷めない中、「CCS Injection Vulnerability」と呼ばれる新たな脆弱性が報告されました。これはOpenSSLのハンドシェイク中に不適切な順序でChange CipherSpecメッセージを挿入することによって、強度の弱い暗号通信へ強制変更することができるというものです。この結果、適切な強度の暗号化が行われずに、通信内容や認証情報などの情報を読み取られたり改ざんされる恐れがあります。

派生プロジェクトの登場

OpenSSLのシェアは極めて高いことから、これらの脆弱性（とくにHeartbleed）の発見はIT業界に大きな衝撃を与えました。HTTPSサイトのうちの17.5%が脆弱性を抱えたままHeartbeat拡張を有効にしていたという報告もあり、その影響力がWebの安全性を根底から覆しかねないものであることがわかります。そのため、この衝撃的な発表を受けて、OpenSSLをフォークした新しいプロジェクトも発足しました。

LibreSSL

「LibreSSL」はThe OpenBSD Projectが立ち上げたプロジェクトで、OpenBSDで利用されているOpenSSLライブラリを置き換えることを目的としています。同プロジェクトでは、OpenSSLの問題として古いシステムをサポートするためにソースコードが肥大化・複雑化している点や、mallocをはじめとするカスタムメモリコールにさまざまな問題を抱えている点などを挙げています。またプロジェクトの管理方法にも問題を抱えており、古いバグが解決されないまま放置されているとも指摘しています。

そこでLibreSSLプロジェクトでは、OpenSSLのコード削減、メモリ管理の標準ライブラリへの置き換えやFIPS規格サポートの廃止、古いバグの修正などを行い、よりシンプルで安全性の高いセキュリティ基盤を構築するとのことです。

BoringSSL

「BoringSSL」はGoogleが立ち上げたプロジェクトで、その目的はおもにGoogle内部での利用を想定したコードベースの構築にあります。Googleでは以前からOpenSSLのコードを検証し、独自に多数のパッチを適用して自社のプロダクトに使用してきましたが、その数が増えるにしたがってパッチを充てる労力だけでも大きな負担になっていたとのことです。そこでいったん本家のOpenSSLから離脱して独自のコードベースを築いたうえで、今後OpenSSLに加えられる変更を取り込んでいく、というスタイルを選んだ結果がBoringSSLというわけです。BoringSSLでは、OpenSSLだけでなくLibreSSLに対する変更も取り込んで行く方針を明らかにしています。

こうした新しい活動に注目が集まる一方で、依然として脆弱性のあるOpenSSLを使い続けているWebサイトも多数存在するとのことで、事態が完全に収束するにはもうしばらく時間がかかりそうです。SD

OpenSSL
http://www.openssl.org/