掲載日： 2014/05/26

ゴールデンウイーク直前に発表され世界中の企業に衝撃を与えたOpenSSLの脆弱性問題。その直後にはApache Strutsにおいても脆弱性が明らかになり、システム管理者からゴールデンウイークのお休みを奪った！とのウワサも…。

いずれも自社のWebサーバが攻撃を受け、個人情報や機密情報などが盗み取られたり、不正送金など直接の被害をもたらす可能性があるだけに、これらを利用している企業においてはすべからく迅速な対応・対策が要求される。

本コンテンツでは、OpenSSLの脆弱性によってどのようなリスクがあるのか、企業はどのように対処すべきなのか…などについて簡単に解説しつつ、次々と明らかになる脆弱性に企業はどのように対応すべきかについても考察してみた。

セキュリティ専業ベンダ：シマンテックによるOpenSSL対策に関するPDF資料もご用意したので是非ご参照いただきたい。

OpenSSL脆弱性がもたらした衝撃の理由

瞬く間に世界中に衝撃が拡がった「OpenSSL」の脆弱性に関するニュース。なぜそんなに大きな騒ぎになっているのかというと、まず採用している企業が多いことが挙げられる。ネット上で公開され無料で利用できることもあり、グーグルやアマゾン、フェイスブックといったグローバル大手IT企業から国内中小企業までそのユーザ数はかなりに上る。

更には、この脆弱性を狙った攻撃がもたらすダメージが、企業の経営を揺るがしかねないほど計り知れないためだ。もともとSSL暗号化技術は高度の秘匿性が求められる通信用に開発されたもの。従って流出する可能性のある情報は、パスワードやクレジットカード情報など重要なものが含まれる。

今回発見された脆弱性では、こうした情報のほか暗号通信データの解読に必要な「鍵」まで漏れてしまう可能性さえ指摘されており、そうなるとすべてが丸裸となってしまう。ECサイトでは第三者が本人になりすまして買い物をしたり、ネットバンキングでは不正送金されてしまったり…と極めて深刻な被害をもたらす恐れがある。ちなみにこの脆弱性は「Heartbleed（心臓出血）」と呼ばれている。

OpenSSLとは？

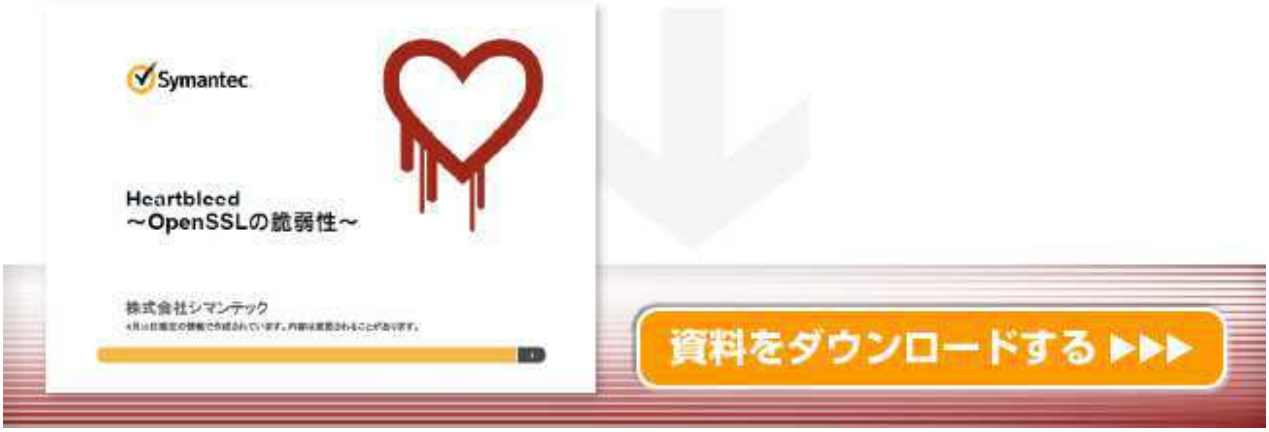
インターネット上でデータを暗号化して送受信するプログラム：SSL（Secure Sockets Layer）の一種。オープンソースのプログラムで、基となるソースコードがネット上で公開されており、世界中の研究者が改良し誰でも無料で利用できる。ネット通販サイトやネットバンキング、会員制サイトなどで個人情報データの送受信やオンライン決済などで幅広く使われている。

OpenSSL脆弱性への対応と、SSLサーバ証明書の再発行について

OpenSSL脆弱性への対応方法については、独立行政法人情報処理推進機構などのホームページで紹介されているが、基本的には「対象サーバのOpenSSLを対策済みバージョン（The OpenSSL ProjectまたはOSベンダに問い合わせた上で）に更新する」か「Heartbeat拡張機能を使用しない設定にする」のいずれかが必要となる。

また前段でご紹介したとおり、通信情報のみならず暗号鍵まで盗み取られている可能性が否定できないため、（SSL/TLS通信やSSLサーバ証明書自体に問題があるわけではない）OpenSSLの更新後SSLサーバ証明書の再発行及び旧証明書の失効が併せて必要となる（業界大手のシマンテックやジオトラストは無償で再発行に応じている）。その上で最後にエンドユーザに対しパスワードなどのリセットを依頼することになる。

なおシマンテック社では、自社のWebサイトが、対策が必要かどうか分からない…という方のために、URL（FQDN）をコピペ入力するだけで脆弱性有無が確認できるツールを用意している。ダウンロード資料に確認方法などが紹介されているので、まずはダウンロードしてご確認を！



セキュリティ空白期間をなくすなら「WAF」がオススメ！

実はその後、OpenSSLの脆弱性に続き、Webアプリケーションプラットフォーム「Apache Struts 2」でも脆弱性が公表されるなど、気の抜けない状況が続いている。無論、すべての脆弱性について可及的速やかに対応しなければならないワケだが、対策中もいつ攻撃されるか分からずシステム管理者にとってビクビクものだ。

そこでオススメしたいのが、OSより上のアプリケーション層を包括的に守ってくれる「WAF（Web Application Firewall）」だ。中でも、シマンテックが提供する「クラウド型WAF」のようなサービスであれば、初期費用を抑えて導入でき、セキュリティ専業会社によるチューニング・運用・保守ごと提供され、専門知識をもたない企業でも安心だ。

クロスサイトスクリプティングやドライブ・バイ・ダウンロード、SQLインジェクションなどの代表的な攻撃手法に加え、今回取り上げたOpenSSLやApache Struts 2の脆弱性を狙った攻撃もブロックするため、脆弱性対策に追われる日々から解放される。

製品・サービスの取扱い企業　合同会社シマンテック・ウェブサイトセキュリティ
掲載企業　合同会社シマンテック・ウェブサイトセキュリティ

印刷日：2014/05/26