SANS SECURING THE HUMAN
NRI SECURE TECHNOLOGIES
OUCH! | 特別号
コンピュータ利用者のためのマンスリー・セキュリティ・アウェアネス・ニュースレター

OUCH!

今月のトピック...

- ハートブリードの脆弱性とは？
- 一般ユーザの対策
- フィッシング攻撃にも注意

ハードブリード（Heartbleed）とは

はじめに

4月7日（月）、SSLプロトコルの実装に幅広く採用されているOpenSSL（オープンSSL）に深刻な脆弱性（ハートブリード）が発見されました。SSLはインターネット上で使用される重要なセキュリティプロトコルの一つです。SSLはインターネット経由の通信を暗号化するだけでなく、オンラインショッピングやオンラインバンキングで接続されるサイトが正規サイトであるかどうかを確認する手段を提供します。今回の特集号では、この脆弱性には、どのような脅威があるのか、またその脅威の被害にあわないようにするには何をすべきか、を説明します。

寄稿者

ジェイク・ウイリアムズ（Jake Williams, **@MalwareJake**, **malwarejake.blogspot.com**）は、CSRgroup Computer Security Consultantsのチーフ・サイエンティストです。またSANSのMemory Forensics (FOR526) やMalware Reverse Engineering (FOR610) の共同執筆者です。

ハートブリードの脆弱性とは？

ハードブリード（Heartbleed：心臓出血）の脆弱性を悪用することで、ハッカーはウェブサーバに接続して、利用者の認証に使われる重要な情報を収集できます。このような情報が第三者に取得されると、正当なユーザでなくても、取得したユーザ名とパスワードを使って、なりすましログインが可能になります。この脆弱性は、2年前から存在していましたが、発見されて公開されたのは、今年の4月7日です。ハートブリードはWindowsやMacなどのパソコンには影響しません。主に影響を受けるのは、FacebookやGmailなどインターネット経由で利用できるウェブサイトやサービスです。インターネット上の全てのサイトに影響するわけではありませんが、多くのサイトに影響します。Lastpassサイトチェックツールを使って利用しているサイトが影響しているか確認することもできます。https://lastpass.com/heartbleed/.

一般ユーザ向け対策

次の手順に従って対策を行ってください。ここに記載する対策は、ハートブリードの脆弱性を悪用されるのを防ぐだけでなく、他の攻撃からも防ぐことができます。

- まず、ハートブリードの脆弱性が存在するOpenSSLを使用しており、すでにパッチを適用しているウェブサイトで、重要なアカウントから順にパスワードを変更してください。ウェブサイトが今回影響を受けたかわからない場合は、とりあえずパスワード変更することを推奨します。これを機会にパスワードを変更して、オンラインのセキュリティレベルを向上させましょう。
- パスワードを変更する場合は、強度の高い、推測されにくいパスワードを使ってください。さらに、ウェブサイトが2段階認証を採用している場合は、有効にし、アカウントをよりセキュアに保ちます。
- アカウント毎に異なるパスワードを使用してください。異なるパスワードを使用することで、一つのウェブサイトが侵害されても、他のウェブサイトのアカウントに影響が及ぶことはありません。パスワードを全て覚えられ

ハードブリード(Heartbleed)とは

ないのが心配な人は、強固パスワードを使っている証拠です。これを機会にパスワードマネージャの利用を推奨します。

- メールクライアントも同じです。OutlookやApple　Mailなどのメールソフトウェアで、SSLを使ってメールサーバに接続している場合、パスワードを変更する必要があります。

ここで述べた手順のさらに詳しい情報は、最後に記載されている「リソース」を参照してください。

あなたの情報を守る最適な方法は、重要なアカウントのパスワードを変更し、アカウント毎に異なる、強固なパスワードを設定してください。

フィッシング攻撃にも注意

残念なことに、このような機会を悪用しようとする人たちもいます。ハートブリードの脆弱性は話題になっており、さまざまなニュースにも取り上げられています。このようなニュースを元に、有名な銀行やオンラインストアなどを装った偽メールを送りつける可能性があるため、十分に注意してください。その他にも、情報セキュリティ会社を装い、ハートブリードの脆弱性を確認するフリーツールの配布という名目で偽メールを送りつける可能性もあります。

企業などになりすましてこのようなメールを送信する手法を、フィッシング攻撃と呼び、決して新しい手法ではありません。攻撃者は、メールを受け取った利用者を誘導してリンクをクリックさせることで、悪意あるサイトにアクセスさせたり、添付ファイルを開かせたりします。このようなフィッシング攻撃が成功してしまうと、パソコンがマルウェアに感染するおそれがあります。そのため、パスワードの変更が必要な場合には、リンクをクリックしてサイトにアクセスするのではなく、ウェブサイトの名前（URLと呼ばれるもの）を直接ブラウザに入力して、パスワードを変更してください。このように、メールなどに記載されたリンクの取扱いを注意するだけでも、フィッシング攻撃にひっかかることなく、正規のウェブサイトに接続することができます。

リソース

対象サイトのチェック:	https://lastpass.com/heartbleed/
OUCH! パスワード:	http://www.securingthehuman.org/ouch/2013#may2013
OUCH! パスワードマネージャ:	http://www.securingthehuman.org/ouch/2013#october2013
OUCH! 2要素認証:	http://www.securingthehuman.org/ouch/2013#august2013
OUCH! フィッシング:	http://www.securingthehuman.org/ouch/2013#february2013
技術解説:	https://www.sans.org/webcasts/openssl-heartbleed-vulnerability-98105

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Translated By: 坂 恵理子, 関取 嘉浩