The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE..

- What Is Heartbleed?
- What Should I Do?
- Beware of Phishing Attacks

Heartbleed - Why Do I Care?

Overview

On Monday April 7th, a serious vulnerability was identified in one of the most popular implementations of the SSL protocol, called OpenSSL. SSL is a very important security protocol used throughout the Internet. Not only does SSL encrypt your online communications, but it helps ensure you are connecting to legitimate websites when you do things like shop or bank online. In this newsletter we give a very simple overview of what this vulnerability means to you and what you can to do protect yourself.

Guest Editor

Jake Williams (**@MalwareJake**; **malwarejake.blogspot.com**) is Chief Scientist at CSRgroup Computer Security Consultants. He is also the coauthor of the Memory Forensics (FOR526) and Malware Reverse Engineering (FOR610) courses at SANS.

What Is Heartbleed?

The Heartbleed vulnerability allows a hacker to connect to a webserver and harvest sensitive information, which may include your login and password. If an attacker were able to harvest such information, they could use that information to log into any of your accounts using the same username and password. While the vulnerability has existed for the past two years, it was only discovered and publicly announced on April 7th. Heartbleed does not affect Windows or Mac computers; it primarily affects websites on the Internet that you use, such as Facebook and Gmail. To make matters more confusing, it does not affect every website on the Internet, but it does impact many of them. You can check if a website you use is or was vulnerable using the Lastpass site checking tool at https://lastpass.com/heartbleed/.

What Should I Do?

There are several steps you can take to protect yourself. Not only will these steps help protect you against the Heartbleed vulnerability, but they will help protect you against many other attacks in the future:

- First, change your passwords on websites that you know were vulnerable and have patched the vulnerability, starting with your most important accounts first. If you do not know if a website was vulnerable, go ahead and change your password anyway. This is a great time to update your passwords and improve your online security.
- Make sure when you update your passwords you use strong, hard-to-guess passwords. In addition, if the website supports something called two-step verification, enable it. This is an additional step that helps make your online account more secure. Finally, if your password has personal questions, we recommend changing the answers.

© The SANS Institute 2014

Heartbleed - Why Do I Care?

- Make sure you are using a separate, unique password for each of your online accounts. That way, even if one website is compromised, all of your other accounts will still be safe. Can't remember all of your passwords? Congratulations, that means you are using strong passwords. We highly recommend you use this opportunity to start using a password manager that stores all of your passwords securely. These are great tools that can not only simplify your online activities, but help make them far more secure.
- Do not forget your email clients. If your email client, such as Outlook or Apple Mail, is using SSL to connect to your mail server, you may need to change those passwords as well.

The best step to protecting yourself is to change your passwords on key accounts and make sure you use a unique, strong password for each one.

Beware of Phishing Attacks

Unfortunately, bad guys are opportunists. They know that Heartbleed has been in the news and a lot of people, including you, have read about it. As such, they will create fake emails that appear to come from legitimate websites you use (such as online banks or stores). They may even pretend to be security companies offering free tools to check for Heartbleed. This tactic (commonly called phishing) is not new. Attackers are attempting to trick you into clicking on links that go to malicious websites or fool you into opening an infected attachment. If you fall victim to these attacks, your computer can be infected. Instead, if you need to change a password, simply type the website's name (often called a URL) into your browser and change your password online. That way, you know you are connecting to the legitimate website.

Resources

Which Sites Are Vulnerable:	https://lastpass.com/heartbleed/
OUCH! Passwords:	http://www.securingthehuman.org/ouch/2013#may2013
OUCH! Password Managers:	http://www.securingthehuman.org/ouch/2013#october2013
OUCH! Two-Step Verification:	http://www.securingthehuman.org/ouch/2013#august2013
OUCH! Phishing:	http://www.securingthehuman.org/ouch/2013#february2013
Technical Details:	https://www.sans.org/webcasts/openssl-heartbleed-vulnerability-98105

License

OUCH! is published by SANS Securing The Human and is distributed under the Creative Commons BY-NC-ND 3.0 license. You are free to share or distribute this newsletter as long as you do not sell or modify the newsletter. For past editions or translated versions, visit www.securingthehuman.org/ouch.

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus