Technology Brief

FOR IT PROFESSIONALS

Orion Labs

Research & Development

April 2014

Follow Orion on LinkedIn:

http://www.linkedin.com/company/1681643

Heartbleed - What is it?

And How Do I Protect Myself?

First, lets begin with some background information written by Aaron Street, featured on the Lawyerist site on April 11, 2014...

So What is Heartbleed?

Lots of websites that require password log-in use an encrypted connection to your browser, called SSL. You can see this when you go to sites that have an "https" website prefix, as opposed to the normal "http" prefix—the "s" means they're using encryption to protect the data sent between you and that website.

One version of SSL is an open-source software called "OpenSSL". For the past two years, the OpenSSL software has had an unknown bug in its code that could have allowed people to see what was supposed to by encrypted data passing between you and the websites using OpenSSL.

"Heartbleed" is just the creative name—given by internet security researchers—to identify the software bug in OpenSSL that allowed for this potential encryption leak.

How Did Heartbleed Happen?

Because OpenSSL is an open-source software project, volunteer software developers around the world are able to submit suggested code edits and fixes, which can later be incorporated into the core software. Two years ago, a German software developer submitted some code fixes—intending to clean up some small software bugs in OpenSSL—and accidentally created a new, unnoticed, bug—now called "Heartbleed".

So What Do I Do Now?

Since that article was written in early April, Heartbleed has been able to be patched by most companies and internet users have been informed to update their passwords, however the problems introduced by Heartbleed are far from over. Below are some steps we suggest taking to ensure you are better protected.

1) Change your passwords. Although many websites have been patched, it is still important to do this.
2) Avoid using the same password across multiple websites. That way, if one password is breached hackers will not be able to jump across and access other accounts such as social media or online banking.
3) Choose a password that is not easy to guess. Passwords should be long, phrase based and involve a balance of different types of characters - including numbers, letters, capitals and even symbols.
4) Carefully setup password change/reset security questions. Typical reset questions are easy to answer and can even be mined from social media pages or the internet. Try coming up with a scheme of answers to these questions that you won't forget (or store securely using a password manager such as LastPass, 1Password, etc.). Many web services also offer "two-factor authentication" for their logins, which we also suggest using.

If you still have questions, we can help. Feel free to contact Orion Support today.