NEWS BRIEF

Presented by **MFL Science & Technology**

What You Need to Know About the Heartbleed Bug

Making waves in the Internet security community is the discovery of the Heartbleed bug, a serious vulnerability that allows hackers to steal personal information that is normally protected by OpenSSL encryption. OpenSSL provides security for Web applications, email, instant messaging and some virtual private networks. According to Internet security services provider Netcraft, about half a million trusted websites are vulnerable to the bug.

Heartbleed Basics

The bug allows anyone on the Internet to read the memory of any applications or websites that use vulnerable versions of OpenSSL. Hackers can exploit the vulnerability to steal four types of data:

1. Encryption keys, which can be used to decrypt protected information
2. User credentials, such as username and passwords
3. Personal information, such as financial details or private emails
4. Other information that they won't have much use for after OpenSSL is updated to a fixed version

Are You Affected?

Chances are this affects you and your business in one way or another. OpenSSL is the most popular cryptographic library in use on the Internet, so it is likely that you use several websites that may have this vulnerability. Unfortunately, websites using the most current versions of OpenSSL (versions 1.0.1 through 1.0.1f) are the ones most likely to be at risk. Earlier versions are not vulnerable.

How Can You Fix the Problem?

OpenSSL has issued a fix for the Heartbleed bug. System administrators, or others who handle the infrastructure and Web server on which your site runs, should update OpenSSL to version 1.0.1g immediately. The update can be found at www.openssl.org. It is also a good practice to notify your customers that you have reacted quickly to fix the vulnerability.

What Should Employees, Friends and Family Do?

Do not advise non-technical employees, family and friends to stay off the Internet entirely. Changing every password they have may be pointless if the website in question is still vulnerable. Websites that are vulnerable will likely contact users to let them know exactly what to do, up to and including changing passwords.

Use this as an opportunity to share the importance of picking strong passwords and using two-factor authentication wherever possible. These methods won't necessarily protect them from a Heartbleed vulnerability, but they increase the overall security of their information now and in the future.

If you would like to discuss Cyber Liability Insurance please contact one of the team.

MFL Science & Technology
INSURANCE BROKERS