Tucker Ellis LLP

The “Heartbleed” Bug and Responding to a Data Security Breach

APRIL 2014

Announced on April 7, 2014, the “Heartbleed” bug represents one of the most significant threats to data security to date. It is estimated that as many as a half million sites, including banking, social media, and e-mail sites, are affected. The “Heartbleed” bug is a flaw within OpenSSL, a cryptographic software used since March 2012 to protect information transmitted over the Internet, including e-mail, instant messaging, and even virtual private networks. OpenSSL is used to secure as many as two-thirds of all encrypted Internet connections.

The “Heartbleed” bug has lurked within the OpenSSL coding since its inception, allowing attackers to slowly, but effectively, draw out information stored in an affected system’s memory. Consequently, an attacker gains access to private information such as login names, passwords, security questions and answers, access tokens, and other forms of encrypted data.

The unsettling reality is that the full extent of the damage caused by the bug is currently unknown, and may not be ascertainable for some time. This is because OpenSSL updates currently available will fail to protect a system user’s information if (s)he continues to use information (e.g., passwords) already obtained by attackers.

Click here to read the Client Alert on addressing the “Heartbleed” bug.