Tucker Ellis | LLP

CLIENT ALERT

THE "HEARTBLEED" BUG AND RESPONDING TO A DATA SECURITY BREACH

APRIL 2014

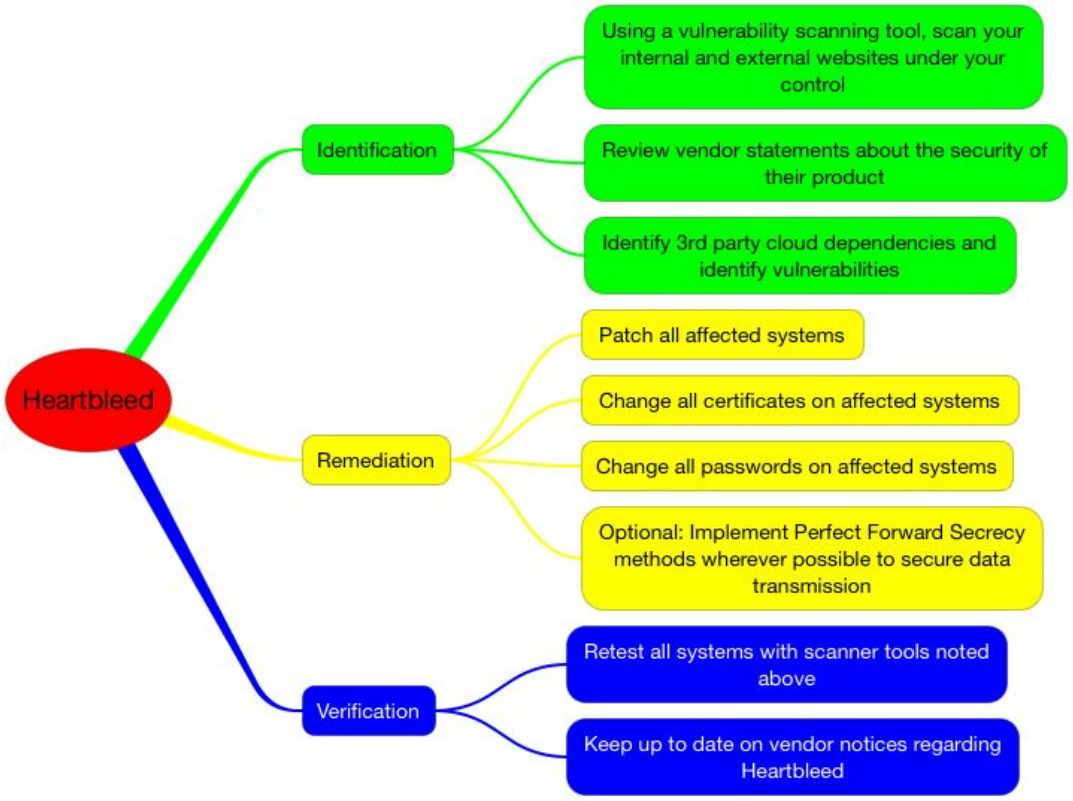
Announced on April 7, 2014, the "Heartbleed" bug represents one of the most significant threats to data security to date. It is estimated that as many as a half million sites, including banking, social media, and e-mail sites, are affected. The "Heartbleed" bug is a flaw within OpenSSL, a cryptographic 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.

ADDRESSING THE "HEARTBLEED" BUG

While the time and resources needed to address the data security threat posed by the "Heartbleed" bug will depend on the configuration and complexity of your computer systems, a conceptual approach for assessing and addressing the task is illustrated below.



BE PREPARED TO RESPOND TO A DATA SECURITY BREACH

From the moment you first learn of the breach:

1. **Obtain as much information as you can about the breach** in order to identify the source(s) and cause(s) of the breach, effectively marshal resources to resolve the problem, and understand your business and legal responsibilities and remedies.
2. **Put your Data Security Response Team to work,** including information technology, legal, risk management, human resources, corporate compliance, and public relations personnel.
3. **Provide timely, but just as important, accurate information** to members of the leadership team, key stakeholders, insurers, key customers, vendors, and partners. Also give timely notifications as required by state and federal law.
4. **Act quickly** to identify and fix the problem, restore company and consumer confidence, and meet legal obligations. The company's Data Security Response Team must be a well-rehearsed rapid response team, trained to act accurately and efficiently.
5. **Document everything.** From the moment you first learn about a breach, it is imperative that you create a record of all steps taken to address and remedy the situation.

UNDERSTANDING THE RISK

The "Heartbleed" bug is an extraordinary data security threat. If affected sites *and their users* fail to proactively respond to this and other data security threats, they risk adverse consequences, such as civil penalties, loss of customer confidence, and increased litigation costs and insurance premiums.

Tucker Ellis's Privacy and Data Security Group assists clients with all aspects of their privacy and data security programs, from creating or updating a data security crisis management plan to ensuring compliance with all applicable state and federal laws and regulations.

ADDITIONAL INFORMATION

For more information, please contact:

ROB HANNA, CHAIR
Privacy & Data Security Group
robert.hanna@tuckerellis.com
216.696.3463

ED TABER
Tucker Ellis LLP Privacy Official
ed.taber@tuckerellis.com
216.696.2365

PAUL JANOWICZ
Privacy & Data Security Group
paul.janowicz@tuckerellis.com
216.696.5787