PUBLICATION

The Heartbleed Bug's Impact on EHR Systems

Authors: Alisa L. Chestler
April 28, 2014

As reported in the media, a serious vulnerability in the popular OpenSSL cryptographic software library, called the Heartbleed bug, was recently discovered. This vulnerability permits the theft of information, including secret keys used to identify service providers, the names and passwords of users, and actual content, that, under normal circumstances, is protected by SSL/TLS encryption. Most health care providers, however, are not aware that many web-based electronic health record (EHR) systems often use OpenSSL's encryption software to secure protected health information (PHI). These web-based systems may be vulnerable to the bug.

Accordingly, for our provider clients, we have two recommendations. First, we recommend that providers contact their vendors to find out (1) whether their system is (or was) subject to the Heartbleed vulnerability and (2) whether the vendor has deployed the fixed version of OpenSSL. Second, we recommend that providers instruct their users and administrators to change their passwords to prevent any unauthorized access. Please note that passwords changed prior to the vendor's installation of the fixed version of OpenSSL are not secure. Providers should also use this opportunity to review their password policies to ensure that they are changed and tested on a routine basis.

More information about the Heartbleed bug can be found here: http://heartbleed.com

This vulnerability has affected several applications and web-based services. If you have questions about the Heartbleed bug or other data security issues, please contact a member of Baker Donelson's Privacy and Information Security Team.