Release Note #89

Topic: Important Heartbleed Bug Information April 24, 2014

General Information:

System Studies Incorporated would like to mitigate possible customer concern regarding the vulnerability of their data on PressureMAP™/PressureWEB™ systems. The concern pertains to the Heartbleed bug that was identified and made public recently. Heartbleed is a flaw in the OpenSSL implementation of the basic cryptographic protocol, know as Secure Sockets Layer (SSL), that secures web communications. SSL basically ensures that no one can eavesdrop while you are visiting a protected site. SSL puts the S in the “https” prefix that appears in the web address when you visit a site that uses a secure, encrypted connection.

Please note that while System Studies Incorporated does not use OpenSSL specifically with our PressureMAP/PressureWEB software, it is installed on the PressureMAP server’s CentOS 5.5 operating system. The version of OpenSSL installed for CentOS 5.5 is 0.9.8e, release 12.el5_4.6. This OpenSSL version DOES NOT CONTAIN the Heartbleed bug, which was first introduced in CentOS Version 6.5.

Operating System Vulnerability:

Some operating system distributions that have shipped with potentially-vulnerable OpenSSL versions:

- Debian Wheezy (stable), OpenSSL 1.0.1e-2+deb7u4
- Ubuntu 12.04.4 LTS, OpenSSL 1.0.1-4ubuntu5.11
- **CentOS 6.5, OpenSSL 1.0.1e-15**
- Fedora 18, OpenSSL 1.0.1e-4
- OpenBSD 5.3 (OpenSSL 1.0.1c 10 May 2012) and 5.4 (OpenSSL 1.0.1c 10 May 2012)
- FreeBSD 10.0 - OpenSSL 1.0.1e 11 Feb 2013
- NetBSD 5.0.2 (OpenSSL 1.0.1e)
- OpenSUSE 12.2 (OpenSSL 1.0.1c)

Vulnerability Status of OpenSSL Versions:

- OpenSSL 1.0.1 through 1.0.1f (inclusive) are vulnerable
- OpenSSL 1.0.1g is NOT vulnerable
- OpenSSL 1.0.0 branch is NOT vulnerable
- OpenSSL 0.9.8 branch is NOT vulnerable

Please note that the Heartbleed bug was introduced to OpenSSL in December 2011 and has been out in the wild since OpenSSL released Version 1.0.1 on March 14, 2012. OpenSSL 1.0.1g, which was released on April 7, 2014, fixes the bug.

For further details regarding Heartbleed, visit http://heartbleed.com.