UPDATE

"Heartbleed" Risk with OpenSSL Does Not Affect Connected Payments

April 10, 2014

Connected Payments is not affected by the "Heartbleed" fault in the OpenSSL product. Connected Payments uses a different SSL system of certificates and keys, and also encrypts data before submitting the packages to the SSL protocol ("double-encryption").

The "Heartbleed" fault itself is not a data "breach" or theft. It is a security risk, since the opening created by this bug could be exploited to compromise confidential information as well as capturing SSL encryption keys and certificate information from a system's OpenSSL implementation. The SSL key information could then be used to expose all transmissions from that system.

Heartbleed affects systems using Codenomicon's popular OpenSSL system for encrypting data transmissions. According to industry estimates, two-thirds of websites operating on the Internet use OpenSSL, including many major commercial sites.

Secure Socket Link (SSL) is a protocol designed to ensure message integrity and protect data transmissions. Contingent upon validation of certificates, keys are agreed and exchanged by the sending and receiving systems, and the data is encrypted and decrypted according to those keys. SSL is used for electronic commerce, electronic mail and FAX, electronic messaging and Web browsing – in fact, in just about any application where data is transmitted.

Keep in mind that Connected Payments double-encrypts the sensitive "track data" portion of the communication, with the specific encoding method dependent upon the PIN pad model and its implementation in the site. But regardless of the encryption method used, the track data would not have been vulnerable to the Heartbleed-like SSL flaw with Connected Payments.

This latest security challenge to the industry demonstrates once again the increasing importance to implementing hardware-based P2Pe encryption as soon as possible. Reinforced with Solidcore to protect the system platforms from invasions, plus proper firewalls to control incoming ***and*** out-going network control, this combination provides the best available protection.