Important Information on SSL Vulnerability

You may have seen reports in the media about a critical vulnerability in the openSSL library that powers SSL functionality on many of the world's leading websites. Code named "Heartbleed", the issue has made front page news and may affect hundreds of thousands of websites worldwide.

SSL stands for "Secure Sockets Layer" and is the protocol that is used by websites to encrypt the transmission of sensitive data such as credit card information.

openSSL is the most common software used to provide SSL functionality on websites. We use openSSL as part of our implementation of SSL.

The "Heartbleed" vulnerability does not affect versions of openSSL prior to 1.0.1.

We can confirm that all of our servers are currently running version **0.9.8e-flps-rhel5** and are therefore **unaffected** by this issue.