



Tech Notice

Worldox[®] is Not Affected by the Heartbleed Vulnerability in OpenSSL

Many of our customers have been asking about the Heartbleed vulnerability in OpenSSL which has recently come to the attention of the public. This vulnerability is the result of programming error in OpenSSL which exposes confidential information such as passwords and session and server keys used for decrypting past and future SSL traffic captured from the server.

Fortunately, all of World Software Corporation's products are NOT affected by this vulnerability. The error does not exist in SSL communications generally, but rather only affected versions of OpenSSL. OpenSSL is a programming library that is typically used on Linux/Unix systems to provide SSL communication for many web servers for banking and web mail sites, etc. Microsoft[®] Windows systems and Windows IIS web servers do not use OpenSSL, Since Worldox Professional, Enterprise, Cloud and Worldox Web products are Windows based systems, they are not affected by this flaw.

As always Worldox will continue to strive to make sure your data remains secure.