Service Bulletin

Security Advisory

No. 20140411-Heartbleed / Revised 04-11-2014

Allworx Products Are Not Vulnerable to "Heartbleed" OpenSSL Heartbeat Extension Attack

Revision 1.0
Last Updated 2014 April 11
For Public Release 2014 April 11

Summary

Allworx has reviewed the implementations of the SSL protocol in all of its products and has verified that Allworx products and the Allworx Portal web site are **not vulnerable** to the "Heartbleed" attacks that were publicized on April 7, 2014.

Affected Products

Vulnerable Products

- None

Products Confirmed Not Vulnerable

- Allworx Servers
- Allworx Phones
- Allworx Software Products
- Allworx PowerFlex switches

Detail

The OpenSSL software library has been incorporated into numerous software products. On April 7, 2014, an attack on OpenSSL 1.0.1 was announced, and dubbed "Heartbleed". Systems running vulnerable code enable anyone to read the memory of systems protected by the OpenSSL software,

and potentially expose secret keys, user names and passwords, or any other content on the vulnerable system.

- This vulnerability has been assigned the Common Vulnerabilities and Exposures (CVE) ID CVE-2014-0160.
- The OpenSSL Security Advisory is at https://www.openssl.org/news/secadv_20140407.txt
- Several useful links and answers have been published at http://heartbleed.com/.

A review of the implementations within Allworx products and the Allworx Portal web site has verified that there is no vulnerability to this attack.

Revision History

Revision 1.0	2014-April-11	Initial public release