Service Bulletin

Security Advisory

No. 20160129-3197/ Revised 01-29-2016

Allworx® products are Not Vulnerable to "SSLv2 doesn't block disabled ciphers" (CVE-2015-3197)

Revision 1.0
Last Updated 2016 January 29
For Public Release 2016 February 01

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 website are **not vulnerable** to the OpenSSL vulnerability CVE-2015-3197 that was announced on 28 January 2016.

Affected Products

Vulnerable Products

- None

Products Not Vulnerable

- Allworx servers
- Allworx IP phones
- Allworx software applications
- Allworx portal

Additional Details

The OpenSSL software library has been incorporated into numerous software products. On January 28, 2016, a "Low" severity vulnerability in OpenSSL 1.0.1 and 1.0.2 was announced. A malicious client can negotiate SSLv2 ciphers that have been disabled on the server and complete SSLv2 handshakes even if all SSLv2 ciphers have been disabled. This vulnerability has been assigned the Common Vulnerabilities and Exposures (CVE) ID CVE-2015-3197.

- The OpenSSL Security Advisory is at http://openssl.org/news/secadv/20160128.txt

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

Recommended Next Steps

Version 8.0.9.5 and earlier of System Software 8.0 incorporate OpenSSL version 1.0.1 software. Version 8.0.10.7 and higher incorporate OpenSSL version 1.0.2 software. Allworx intends to release Versions 8.0.18.x and 8.1.3.x on or around 25 February 2016, containing OpenSSL 1.0.2f, which addresses the vulnerability described here (even though the System Software is not vulnerable).

Sites concerned about this or other vulnerabilities should:

- Procure and install SSL certificates on the Allworx Connect™ servers

Revision History

Revision 1.0	2016-February-01	Initial public release