Service Bulletin
Security Advisory

No. 20161110-7054/ Revised 11-17-2016

Allworx® products are Not Vulnerable to the vulnerabilities announced by the OpenSSL Security Advisory of November 10, 2016

Revision 1.0
Last Updated 2016 November 17
For Public Release 2016 November 18

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 vulnerabilities that were announced on 10 November 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 November 10th, 2016, the following vulnerabilities were announced in OpenSSL 1.1.0:

- **ChaCha20/Poly1305 heap-buffer-overflow (CVE-2016-7054)**
  Severity Level: High
  TLS connections using *-CHACHA20-POLY1305 ciphersuites are susceptible to a DoS attack by corrupting larger payloads..

- **CMS Null dereference (CVE-2016-7053)**
  Severity Level: Moderate
  Applications parsing invalid CMS structures can crash with a NULL pointer dereference.
- **Montgomery multiplication may produce incorrect results (CVE-2016-7055)**
  Severity Level: Low
  There is a carry propagating bug in the Broadwell-specific Montgomery multiplication procedure that handles input lengths divisible by, but longer than 256 bits.

Additional details about these vulnerabilities may be found in the OpenSSL Security Advisory at https://www.openssl.org/news/secadv/20161110.txt.

A review of the implementations within Allworx products and the Allworx Portal website has verified that there are no vulnerabilities to these attacks.

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.

Sites concerned about these or other vulnerabilities should:

- Regularly update the Allworx System Software to the most recent version available on the Allworx portal
- Procure and install SSL certificates on the Allworx Connect™ servers

Revision History

Revision 1.0	2016-November-18	Initial public release