Service Bulletin
Security Advisory

No. 20171207-3737/ Revised December 7, 2017

Allworx® products are Not Vulnerable to the vulnerabilities announced by the OpenSSL Security Advisory of December 7, 2017

Revision 1.0
Last Updated December 7, 2017
For Public Release December 7, 2017

Summary

Allworx has reviewed the implementations of the SSL protocol in all its products and has verified that Allworx products and the Allworx Portal website are **not vulnerable** to the OpenSSL vulnerabilities that were announced on December 7, 2017.

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 December 7, 2017, the following vulnerabilities were announced in OpenSSL 1.0.2 and 1.1.0:

- **Read/write after SSL object in error state (CVE-2017-3737)**
  Severity Level: Moderate
  OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit

handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it oes not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer.

In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error.

- **rsaz_1024_mul_avx2 overflow bug on x86_64 (CVE-2017-3738)**
  Severity Level: Low
  There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701.

  This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation).

Additional details about these vulnerabilities may be found in the OpenSSL Security Advisory at https://www.openssl.org/news/secadv/20171207.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	December 7, 2017	Initial public release