Service Bulletin
Security Advisory

No. 20160301-0800/ Revised 03-02-2016

Allworx® products are Not Vulnerable to the vulnerabilities announced by the OpenSSL Security Advisory of March 01, 2016

Revision 1.0
Last Updated 2016 March 02
For Public Release 2016 March 03

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 01 March 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 March 1st, 2016, the following vulnerabilities were announced in OpenSSL 1.0.1 and 1.0.2:

- **Cross-protocol attack on TLS using SSLv2 (DROWN) (CVE-2016-0800)**
  Severity Level: High
  A cross-protocol attack was discovered that could lead to decryption of TLS sessions by using a server supporting SSLv2 and EXPORT cipher suites as a Bleichenbacher RSA padding oracle.

- **Double-free in DSA code (CVE-2016-0705)**
  Severity Level: Low
  A double free bug was discovered when OpenSSL parses malformed DSA private key.
- **Memory leak in SRP database lookups (CVE-2016-0798)**
  Severity Level: Low
  SRP servers that configure a secret seed to hide valid login information are vulnerable to a memory leak.
- **BN_hex2bn/BN_dec2bn NULL pointer deref/heap corruption (CVE-2016-0797)**
  Severity Level: Low
  In certain cases, the BN_hex2bn and BN_dec2bn functions can allocate memory to an insufficiently sized field leading to heap corruption.
- **Fix memory issues in BIO_*printf functions (CVE-2016-0799)**
  Severity Level: Low
  The internal fmtstr function used in processing internal debug strings can overflow when processing very long strings.
- **Side channel attack on modular exponentiation (CVE-2016-0702)**
  Severity Level: Low
  A side-channel attack was found which makes use of cache-bank conflicts on the Intel Sandy-Bridge microarchitecture which could lead to the recovery of RSA keys.
- **Divide-and-conquer session key recovery in SSLv2 (CVE-2016-0703)**
  Severity Level: High
  If clear-key bytes are present for SSLv2 cyphers, an eavesdropper may be able to determine the SSLv2 master-key.
- **Bleichenbacher oracle in SSLv2 (CVE-2016-0704)**
  Severity Level: Moderate
  Bytes can be overwritten in the master-key when applying Bleichenbacher protection for export cipher suites.

Additional details about these vulnerabilities may be found in the OpenSSL Security Advisory at http://openssl.org/news/secadv/20160301.txt.

A review of the implementations within Allworx products and the Allworx Portal website has verified that there are no vulnerabilities to these attacks. In particular, these products do not support SSLv2.

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 8.0.19.x and 8.1.4.x on or around 31 March 2016, containing OpenSSL 1.0.2g, which addresses the vulnerabilities described here (even though the System Software is not vulnerable).

Sites concerned about this 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-March-02	Initial public release