Service Bulletin
Security Advisory

No. 20160922-6304/ Revised 09-27-2016

Allworx® products are Vulnerable to one or more of the vulnerabilities announced by the OpenSSL Security Advisory of 22 September 22 2016

Revision 1.0
Last Updated 27 September 2016
For Public Release 28 September 2016

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 **vulnerable** to one or more of the vulnerabilities that were announced on 22 September 2016.

Additionally, OpenSSL announced additional vulnerabilities on 26 September 2016 that were introduced by the fixes they released in response to the 22 September announcement. Allworx products are **not vulnerable** to these additional vulnerabilities.

Affected Products

Vulnerable Products

- Allworx servers running release 8.0 or 8.1

Products Not Vulnerable

- Allworx IP phones
- Allworx software applications
- Allworx portal

Additional Details

The OpenSSL software library has been incorporated into numerous software products. On 22 September 2016, the following vulnerabilities were announced in OpenSSL:

- **OCSP Status Request extension unbounded memory growth (CVE-2016-6304)**
  Severity Level: High
  A malicious client can send an excessively large OCSP Status Request extension. If that client continually requests renegotiation, sending a large OCSP Status Request extension each time, then there will be unbounded memory growth on the server. This will eventually lead to a Denial of Service attack through memory exhaustion. Servers with a default configuration are vulnerable even if they do not support OCSP.

- **SSL_peek() hang on empty record (CVE-2016-6305)**
  Severity Level: Moderate
  OpenSSL 1.1.0 SSL/TLS will hang during a call to SSL_peek() if the peer sends an empty record. This could be exploited by a malicious peer in a Denial of Service attack.

- **SWEET32 Mitigation (CVE-2016-2183)**
  Severity Level: Low
  SWEET32 (https://sweet32.info) is an attack on older block cipher algorithms that use a block size of 64 bits. In mitigation for the SWEET32 attack DES based ciphersuites have been moved from the HIGH cipherstring group to MEDIUM in OpenSSL 1.0.1 and OpenSSL 1.0.2.

- **OOB write in MDC2_Update() (CVE-2016-6303)**
  Severity Level: Low
  An overflow can occur in MDC2_Update() either if called directly or through the EVP_DigestUpdate() function using MDC2.

- **Malformed SHA512 ticket DoS (CVE-2016-6302)**
  Severity Level: Low
  If a server uses SHA512 for TLS session ticket HMAC it is vulnerable to a DoS attack where a malformed ticket will result in an OOB read which will ultimately crash.

- **OOB write in BN_bn2dec() (CVE-2016-2182)**
  Severity Level: Low
  The function BN_bn2dec() does not check the return value of BN_div_word(). This can cause an OOB write if an application uses this function with an overly large BIGNUM.

- **OOB read in TS_OBJ_print_bio() (CVE-2016-2180)**
  Severity Level: Low
  The function TS_OBJ_print_bio() misuses OBJ_obj2txt(): the return value is the total length the OID text representation would use and not the amount of data written.

- **Pointer arithmetic undefined behaviour (CVE-2016-2177)**
  Severity Level: Low
  Avoid some undefined pointer arithmetic behavior.

- **Constant time flag not preserved in DSA signing (CVE-2016-2178)**
  Severity Level: Low
  Operations in the DSA signing algorithm should run in constant time in order to avoid side channel attacks.

- **DTLS buffered message DoS (CVE-2016-2179)**
  Severity Level: Low

In a DTLS connection where handshake messages are delivered out-of-order those messages that OpenSSL is not yet ready to process will be buffered for later use.

- **DTLS replay protection DoS (CVE-2016-2181)**
  Severity Level: Low
  A flaw in the DTLS replay attack protection mechanism means that records that arrive for future epochs update the replay protection "window" before the MAC for the record has been validated.
- **Certificate message OOB reads (CVE-2016-6306)**
  Severity Level: Low
  In OpenSSL 1.0.2 and earlier some missing message length checks can result in OOB reads of up to 2 bytes beyond an allocated buffer.
- **Excessive allocation of memory in tls_get_message_header() (CVE-2016-6307)**
  Severity Level: Low
  A TLS message includes 3 bytes for its length in the header for the message, which is allocated prior to the excessive message length check.
- **Excessive allocation of memory in dtls1_preprocess_fragment() (CVE-2016-6308)**
  Severity Level: Low
  This issue is very similar to CVE-2016-6307. The underlying defect is different but the security analysis and impacts are the same except that it impacts DTLS.

Additional details about these vulnerabilities may be found in the OpenSSL Security Advisory at https://www.openssl.org/news/secadv/20160922.txt.

A review of the implementations within Allworx products and the Allworx Portal website has verified that Allworx servers are **vulnerable** to High severity issue **CVE-2016-6304**.

On 26 September 2016, the following vulnerabilities were announced in OpenSSL:

- **Fix Use After Free for large message sizes (CVE-2016-6309)**
  Severity Level: Critical
  This issue only affects OpenSSL 1.1.0a, released on 22 September 2016. The patch applied to address CVE-2016-6307 resulted in an issue where if a message larger than approximately 16k is received then the underlying buffer to store the incoming message is reallocated and moved.
- **Missing CRL sanity check (CVE-2016-7052)**
  Severity Level: High
  This issue only affects OpenSSL 1.0.2i, released on 22 September 2016. A bug fix which included a CRL sanity check was added to OpenSSL 1.1.0 but was omitted from OpenSSL 1.0.2i.

Additional details about these vulnerabilities may be found in the OpenSSL Security Advisory at https://www.openssl.org/news/secadv/20160926.txt.

A review of the implementations within Allworx products and the Allworx Portal website has verified that they are **not vulnerable** to these attacks, as no products were released with the OpenSSL software of 22 September 2016.

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 does not use OpenSSL version 1.1.0 software.

Allworx intends to release Versions 8.0.25.x and 8.1.10.x on or around 06 October 2016, containing OpenSSL 1.0.2j, which addresses all of the vulnerabilities described here. Allworx recommends that systems running System Software 8.0 or 8.1 upgrade to this patch release.

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	28 September 2016	Initial public release