Service Bulletin

Security Advisory

No. 20160502-2108/ Revised 05-03-2016

Allworx® products are Not Vulnerable to the vulnerabilities announced by the OpenSSL Security Advisory of May 02, 2016

Revision 1.0
Last Updated 2016 May 03
For Public Release 2016 May 04

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 02 May 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 May 2nd, 2016, the following vulnerabilities were announced in OpenSSL 1.0.1 and 1.0.2:

- **Memory corruption in the ASN.1 encoder (CVE-2016-2108)**
  Severity Level: High
  If an application deserializes untrusted ASN.1 structures containing an ANY field, and later reserializes them, an attacker may be able to trigger an out-of-bounds write. This has been shown to cause memory corruption.

- **Padding oracle in AES-NI CBC MAC check (CVE-2016-2107)**
  Severity Level: High
  A MITM attacker can use a padding oracle attack to decrypt traffic when the connection uses an AES CBC cipher and the server support AES-NI.
- **EVP_EncodeUpdate overflow (CVE-2016-2105)**
  Severity Level: Low
  An overflow can occur in the EVP_EncodeUpdate() function which is used for Base 64 encoding of binary data, resulting in heap corruption.
- **EVP_EncryptUpdate overflow (CVE-2016-2106)**
  Severity Level: Low
  An overflow can occur in the EVP_EncryptUpdate(), resulting in heap corruption.
- **ASN.1 BIO excessive memory allocation (CVE-2016-2109)**
  Severity Level: Low
  When ASN.1 data is read from a BIO using functions such as d2i_CMS_bio() a short invalid encoding can cause allocation of large amounts of memory potentially consuming excessive resources or exhausting memory.
- **EBCDIC overread (CVE-2016-2176)**
  Severity Level: Low
  ASN1 Strings that are over 1024 bytes can cause an overread in applications using the X509_NAME_oneline() function on EBCDIC systems

Additional details about these vulnerabilities may be found in the OpenSSL Security Advisory at http://openssl.org/news/secadv/20160503.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. Allworx intends to release Versions 8.0.21.x and 8.1.6.x on or around 02 June 2016, containing OpenSSL 1.0.2h, which addresses the vulnerabilities described here (even though the System Software is not vulnerable).

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-May-03	Initial public release