Service Bulletin
Security Advisory

No. 20190304-1559/ Revised March 4, 2019

Allworx® products are not vulnerable to the vulnerability announced by the OpenSSL Security Advisory of February 26, 2019

Revision 1.0
Last Updated March 4, 2019
For Public Release March 27, 2019

Summary

Allworx has reviewed the implementations of the SSL protocol in all its products and has verified that Allworx servers are **not vulnerable** to the OpenSSL vulnerability announced on February 26, 2019. This vulnerability (CVE-2019-1559) is described as having a moderate severity by the OpenSSL organization. The Allworx servers, Allworx IP phones, Allworx Portal, and Allworx software applications are not vulnerable.

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 February 26, 2019, the following vulnerability was announced in OpenSSL 1.0.2:

0-byte record padding oracle (CVE-2019-1559)
Severity Level: Moderate
If an application encounters a fatal protocol error and then calls SSL_shutdown() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling application if a 0

byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MAC. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amounts to a padding oracle that could be used to decrypt data.

In order for this to be exploitable "non-stitched" ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do anyway).

Additional details about these vulnerabilities may be found in the OpenSSL Security Advisory at https://www.openssl.org/news/secadv/20190226.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. Versions 8.0.10.7 through any patch version of 8.4 (e.g., 8.4.6.3) incorporate OpenSSL version 1.0.2 software. Version 8.5 and higher incorporate OpenSSL version 1.1.1 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	March 4, 2019	Initial public release