



Service Bulletin Security Advisory

No. 20170216-3733/ Revised February 21, 2017

Allworx[®] products are Not Vulnerable to the vulnerabilities announced by the OpenSSL Security Advisory of February 16, 2017

Revision 1.0

Last Updated February 21, 2017

For Public Release February 21, 2017

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 February 16, 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 February 16, 2017, the following vulnerabilities were announced in OpenSSL 1.1.0:

- **Encrypt-Then-Mac renegotiation crash (CVE-2017-3733)**

Severity Level: High

During a renegotiation handshake if the Encrypt-Then-Mac extension is negotiated where it was not in the original handshake (or vice-versa) then this can cause OpenSSL to crash (dependent on ciphersuite). Both clients and servers are affected.

Toll Free: 1 866 ALLWORX • 585 421 3850 • www.allworx.com

© 2017 Allworx Corp, a Windstream Company. All rights reserved.



Additional details about these vulnerabilities may be found in the OpenSSL Security Advisory at <https://www.openssl.org/news/secadv/20170216.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	February 21, 2017	Initial public release
--------------	-------------------	------------------------