Service Bulletin

Security Advisory

No. 20151204-3196/ Revised 12-08-2015

Allworx Products are Not Vulnerable to "Race condition handling PSK identify" (CVE-2015-3196)

Revision 1.0
Last Updated 2015 December 08
For Public Release 2015 December 09

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 web site are **not vulnerable** to the OpenSSL vulnerability CVE-2015-3196 that was announced on December 3, 2015.

Affected Products

Vulnerable Products

- None

Products Confirmed Not Vulnerable

- Allworx Servers
- Allworx Phones
- Allworx Software Products

Detail

The OpenSSL software library has been incorporated into numerous software products. On December 3, 2015, a "low" severity vulnerability in OpenSSL 1.0.0, 1.0.1 and 1.0.2 was announced. Systems running vulnerable code can encounter a race condition leading to a double free of PSK identity data that has been received. This vulnerability has been assigned the Common Vulnerabilities and Exposures (CVE) ID CVE-2015-3196.

- The OpenSSL Security Advisory is at https://www.openssl.org/news/secadv/20151203.txt

A review of the implementations within Allworx products and the Allworx Portal web site has verified that there is no vulnerability to this attack.

Versions 8.0.9.5 and earlier of System Software 8.0 incorporate OpenSSL version 1.0.1 software. Version 8.0.10.7 and later incorporate OpenSSL version 1.0.2d software which addresses this vulnerability.

Revision History

Revision 1.0	2015-December-09	Initial public release