Service Bulletin

Security Advisory

No. 20150717-1793/ Revised 07-17-2015

Allworx Products are Not Vulnerable to OpenSSL Alternative chains certificate forgery (CVE-2015-1793)

Revision 1.0
Last Updated 2015 July 17
For Public Release 2015 July 20

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-2015-1793 that was announced on July 11, 2015.

Affected Products

Vulnerable Products

- None

Products Confirmed Not Vulnerable

- Allworx Servers
- Allworx Phones
- Allworx Software Products
- Allworx PowerFlex switches

Detail

The OpenSSL software library has been incorporated into numerous software products. On July 11, 2015, a vulnerability in OpenSSL 1.0.1n and 1.0.1o was announced. Systems running vulnerable code enable attackers to cause certain checks on untrusted certificates to be bypassed, enabling them to use a valid leaf certificate to act as a Certificate Authority and "issue" an invalid certificate.

- This vulnerability has been assigned the Common Vulnerabilities and Exposures (CVE) ID CVE-2015-1793.
- The OpenSSL Security Advisory is at https://www.openssl.org/news/secadv_20150709.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.

Allworx System Software 8.0 incorporates OpenSSL version 1.0.1 software. However, no releases were made containing OpenSSL versions 1.0.1n or 1.0.1o. Version 8.0.7.6 (released 2015-June-18) contains version 1.0.1m, and Version 8.0.8.6 (released 2015-July-16) contains version 1.0.1p, which contains the fix for this vulnerability.

Revision History

Revision 1.0	2015-July-20	Initial public release