Service Bulletin

Security Advisory

No. 20151204-3193/ Revised 12-08-2015

Allworx Products are Not Vulnerable to "BN_mod_exp may produce incorrect results on x86_64" (CVE-2015-3193)

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-2015-3193 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 "Moderate" severity vulnerability in OpenSSL 1.0.2 was announced. This vulnerability is a carry propagating bug in the x86_64 Montgomery squaring procedure. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline.

- This vulnerability has been assigned the Common Vulnerabilities and Exposures (CVE) ID CVE-2015-3193.
- 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 1.0.2 software. Allworx intends to release Version 8.0.15.x on or around 17 December, 2015, containing OpenSSL 1.0.2e, which addresses the vulnerability described here (even though the System Software is not vulnerable).

Revision History

Revision 1.0	2015-December-09	Initial public release