Service Bulletin
Security Advisory

No. 20171102-3735/ Revised November 2, 2017

Allworx® products are vulnerable to one of the vulnerabilities announced by the OpenSSL Security Advisory of November 2, 2017

Revision 1.0
Last Updated November 2, 2017
For Public Release November 2, 2017

Summary

Allworx has reviewed the implementations of the SSL protocol in all its products and has verified that Allworx servers are **vulnerable** to one of the OpenSSL vulnerabilities announced on November 2, 2017. This vulnerability (CVE-2017-3735) is described as having a low severity by the OpenSSL organization. The Allworx Portal, Allworx IP Phones, and Allworx software applications are not vulnerable.

No Allworx products are vulnerable to CVE-2017-3736.

Affected Products

Vulnerable Products

- Allworx Servers

Products Not Vulnerable

- Allworx IP phones
- Allworx software applications
- Allworx portal

Additional Details

The OpenSSL software library has been incorporated into numerous software products. On November 2, 2017, the following vulnerabilities were announced in OpenSSL 1.0.2m and 1.1.0g.

- **Malformed X.509 IPAddressFamily could cause OOB read (CVE-2017-3735)**
  Severity Level: Low

If an X.509 certificate has a malformed IPAddressFamily extension, OpenSSL could do a one-byte buffer overread. The most likely result would be an erroneous display of the certificate in text format.

- **bn_sqrx8x_internal carry bug on x86_64 (CVE-2017-3736)**
  Severity Level: Moderate
  There is a carry propagating bug in the x86_64 Montgomery squaring procedure. No EC algorithms are affected. 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. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients.

  This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.

Additional details about these vulnerabilities may be found in the OpenSSL Security Advisory at https://www.openssl.org/news/secadv/20171102.txt.

Recommended Next Steps

Allworx System Software Version 8.0.10.7 and higher incorporate OpenSSL version 1.0.2 software. Allworx intends to release Versions 8.2.10.x in January, containing OpenSSL 1.0.2m, which addresses the vulnerabilities described here.

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	November 2, 2017	Initial public release