Service Bulletin
Security Advisory

No. 20160129-0701/ Revised 01-29-2016

Allworx® servers are Vulnerable to “DH small subgroups” (CVE-2016-0701)

Revision 1.0
Last Updated 2016 January 29
For Public Release 2016 February 01

Summary

Allworx has reviewed the implementations of the SSL protocol in all of its products and has verified that Allworx servers **are vulnerable** to the OpenSSL vulnerability CVE-2016-0701 that was announced on January 28, 2016. Other Allworx products and the Allworx Portal website are **not vulnerable** to this vulnerability.

Affected Products

Vulnerable Products

- Allworx servers running Release 8.0.10.7 or later

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 January 28, 2016, a “High” severity vulnerability in OpenSSL 1.0.2 was announced which may result in servers using weak encryption parameters (Diffie-Hellman parameters based on unsafe primes). An attacker could perform multiple SSL handshakes to discover a private key component, and then use that private key to conduct a man-in-the-middle active attack on a subsequent connection between a user and a server. This vulnerability has been assigned the Common Vulnerabilities and Exposures (CVE) ID CVE-2016-0701.

- The OpenSSL Security Advisory is at http://openssl.org/news/secadv/20160128.txt

A review of the implementations within Allworx products and the Allworx Portal website has verified that Allworx servers running the following System Software releases are vulnerable to this vulnerability:

- System Software 8.0: Release 8.0.10.7 or higher
- System Software 8.1: Release 8.1.2.7

Recommended Next Steps

Version 8.0.10.7 and higher incorporate OpenSSL version 1.0.2 software. Allworx intends to release Versions 8.0.18.x and 8.1.3.x on or around 25 February 2016, containing OpenSSL 1.0.2f, which addresses the vulnerability described here.

Sites concerned about active man-in-the-middle attacks should:

- Avoid this vulnerability by installing Allworx System Software Release 8.0.18.x or Release 8.1.3.x when it is available.
- Procure and install SSL certificates on the Allworx Connect™ servers.

Revision History

Revision 1.0	2016-February-01	Initial public release