Service Bulletin

Security Advisory

No. 20170127-3731 / Revised 01-27-2017

Allworx® products are not vulnerable to the vulnerabilities announced in the OpenSSL Security Advisory of January 26, 2017

Revision 1.0
Last Updated 2017 January 27
For Public Release 2017 January 27

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 website are **not vulnerable** to the OpenSSL vulnerabilities that were announced on 26 January 2017.

Affected Products

Vulnerable Products

- None

Products Not Vulnerable

- Allworx servers
- Allworx IP phones
- Allworx software applications
- Allworx Portal website

Additional Details

The OpenSSL software library has been incorporated into numerous software products. On January 26th, 2017, the following vulnerabilities were announced:

- **Truncated packet could crash via OOB read (CVE-2017-3731)**
  Severity Level: Moderate
  Affected OpenSSL Versions: 1.1.0, 1.0.2
  If an SSL/TLS server or client is running on a 32-bit host, and a specific cipher is being used, then a

truncated packet can cause that server or client to perform an out-of-bounds read, usually resulting in a crash.

- **Bad (EC)DHE parameters cause a client crash (CVE-2017-3730)**
  Severity Level: Moderate
  Affected OpenSSL Versions: 1.1.0
  If a malicious server supplies bad parameters for a DHE or ECDHE key exchange then this can result in the client attempting to dereference a NULL pointer leading to a client crash. This could be exploited in a Denial of Service attack.

- **BN_mod_exp may produce incorrect results on x86_64 (CVE-2017-3732)**
  Severity Level: Moderate
  Affected OpenSSL Versions: 1.1.0, 1.0.2
  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. For example this can occur by default in OpenSSL DHE based SSL/TLS ciphersuites. Note: This issue is very similar to CVE-2015-3193 but must be treated as a separate problem.

- **Montgomery multiplication may produce incorrect results (CVE-2016-7055)**
  Severity Level: Low
  Affected OpenSSL Versions: 1.1.0, 1.0.2
  This issue was previously fixed in 1.1.0c and covered in security advisory
  https://www.openssl.org/news/secadv/20161110.txt

Additional details about these vulnerabilities may be found in the OpenSSL Security Advisory at https://www.openssl.org/news/secadv/20170126.txt.

A review of the implementations within Allworx products and the Allworx Portal website has verified that there are no vulnerabilities to these attacks.

Recommended Next Steps

Version 8.0.9.5 and earlier of System Software 8.0 incorporate OpenSSL version 1.0.1 software. Version 8.0.10.7 and higher incorporate OpenSSL version 1.0.2 software.

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	2017-January-27	Initial public release