Service Bulletin
Security Advisory

No. 20180327-0739/ Revised March 27, 2018

Allworx® products are Not Vulnerable to the vulnerabilities announced by the OpenSSL Security Advisory of March 27, 2018

Revision 1.0
Last Updated March 27, 2018
For Public Release March 27, 2018

Summary

Allworx has reviewed the implementations of the SSL protocol in all its products and has verified that Allworx products and the Allworx Portal website are **not vulnerable** to the OpenSSL vulnerabilities that were announced on March 27, 2018.

Affected Products

Vulnerable Products

- None

Products Not Vulnerable

- Allworx servers
- Allworx IP phones
- Allworx software applications
- Allworx portal

Additional Details

The OpenSSL software library has been incorporated into numerous software products. On March 27, 2018, the following vulnerabilities were announced in OpenSSL 1.0.2 and 1.1.0:

- **Constructed ASN.1 types with a recursive definition could exceed the stack (CVE-2018-0739)**
  Severity Level: Moderate
  Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is

considered safe.

- **Incorrect CRYPTO_memcmp on HP-UX PA-RISC (CVE-2018-0733)**
  Severity Level: Moderate
  Because of an implementation bug the PA-RISC CRYPTO_memcmp function is effectively reduced to only comparing the least significant bit of each byte. This allows an attacker to forge messages that would be considered as authenticated in an amount of tries lower than that guaranteed by the security claims of the scheme. The module can only be compiled by the HP-UX assembler, so that only HP-UX PA-RISC targets are affected.

- **rsaz_1024_mul_avx2 overflow bug on x86_64 (CVE-2017-3738)**
  Severity Level: Low
  This issue has been reported in a previous OpenSSL security advisory and a fix was provided for OpenSSL 1.0.2. Due to the low severity no fix was released at that time for OpenSSL 1.1.0. The fix is now available in OpenSSL 1.1.0h.

  There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. 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 DH1024 are considered just feasible, 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 significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701.

  This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation).

  Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193.

Additional details about these vulnerabilities may be found in the OpenSSL Security Advisory at https://www.openssl.org/news/secadv/20180327.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	March 27, 2018	Initial public release