Service Bulletin

Security Advisory

No. 20211216-0001/ Revised December 29, 2021

Allworx® products are not vulnerable to Apache log4j attacks

Revision: C

Last Updated: December 29, 2021

First Public Release: December 16, 2021

Summary

In light of recently discovered vulnerabilities in the Apache log4j library:

CVE-2021-44228

CVE-2021-44832

CVE-2021-45046

CVE-2021-45105

CVE-2021-4104

Allworx has reviewed its products' implementations and has verified that **no Allworx products are vulnerable to these attacks**.

Affected Products

Vulnerable Products

- None

Products Not Vulnerable

- Allworx servers (Connect series, Connect Vx, X-series) – no use of log4j library
- Allworx IP phones (Verge 9300 series, 9200 series, 9100 series) – no use of log4j library
- Allworx Portal – no use of log4j library

- Allworx software applications – no use of log4j library:
  - Interact, Interact Softphone
  - Reach
  - View
  - Call Assistant
  - OfficeSafe
- Allworx software applications – using log4j library:
  - Migrate

Additional Details

An adversary can exploit the CVE-2021-44228, CVE-2021-45046, and CVE-2021-45105 vulnerabilities by submitting a specially crafted request to a vulnerable application, causing that application to generate a log message causing the application to (a) execute arbitrary code loaded from an LDAP server, or (b) suffer an infinite recursion resulting in denial of service. Apache log4j versions from 2.0-beta9 through 2.12.1 and 2.13.0 through 2.16.0 are affected.

A lower-severity CVE-2021-4104 vulnerability exists for Apache log4j 1.2 with logging configuration including the JMSAppender feature (which is not the default).

The only Allworx product using the Apache log4j library is the Allworx Migrate application.

It is not vulnerable for multiple reasons:

- Migrate is an end-user interactive application that does not expose any external-facing endpoint through which an adversary could submit crafted log messages. All Migrate log messages are derived from communication with the Allworx server, not from any user- or network-supplied information.
- Migrate's current release incorporates log4j version 1.2.17, which is not vulnerable to CVE-2021-44228, CVE-2021-44832, CVE-2021-45046, or CVE-2021-45105. Migrate would only be vulnerable to CVE-2021-4104 if it was configured to use the JMSAppender feature, and it is not configured that way.
- These vulnerabilities require the log4j configuration to include the JndiLookup class, which Migrate's configuration does not include.

A future release of Allworx Migrate will incorporate an updated Apache log4j library with version at least 2.17.1.

Revision History

Revision A	December 16, 2021	Initial public release
Revision B	December 20, 2021	Not vulnerable to CVE-2021-45105 infinite recursion vulnerability either.
Revision C	December 29, 2021	Not vulnerable to CVE-2021-44832 remote code execution attack either.