LakePharma DPM Enterprise Version 3.44.0 Security Whitepaper

February 2019

I. Introduction

LakePharma DPM Enterprise Version 3.44.0 is a data-management web application developed for LakePharma, Inc. By US-based software company RENKOM. The DPM is highly customizable by the end user, and new functionalities are under continuous development by RENKOM.

II. Architecture and Design

- The LakePharma DPM is an entirely cloud-based web application hosted on Amazon Web Services (AWS). The application is developed primarily in Zend Framework with database storage in MySQL (AWS RDS Instances).

III. Access Control

- The webserver is not exposed to the world and is only accessible via a bastion host on the same secure subnet. SSH access to the bastion host is restricted to IPs associated with the development team.
- The MySQL database is not exposed to the world and can only be accessed by machines in the same secure subnet (IE the webserver).

IV. Authentication

- Application users are required to have a password that includes both numbers and letters and is 8-23 characters long.
- Users are required to change their password every year.
- Multi-Factor Authentication can be enabled for any user.
- Application administrators are required to have Multi-Factor Authentication enabled.
- Users are able to securely recover their username and password.

V. Configuration Management

- System hardening has been performed on production systems
- There is a secure build process. Development is performed by an ISO 27001:2013 certified company. The development team utilizes website filtering and reviews user access rights and group policies regularly. Random audits of USB/storage devides are performed. Security Authentication Control has been implemented on JIRA and the private Github server, and activity logging and monitoring of Github and JIRA are carried out on a monthly basis.

VI. Cryptography

- All Database (MySQL) data is protected with encryption at rest.
- All application resources are encrypted through 256-bit TLS encryption.

VII. Patch Management

- Patches are deployed via GIT and regression testing of all application functionality occurs after every patch

VIII. Proactive Monitoring

- DPM Contains an extensive audit trail detailing all created, edited and deleted information by all users including administrative actions.

- System logs are rotated nightly and stored on a Zabbix server for nightly review and analysis by the DPM development team. Email alerts are sent to the development team by the Zabbix server if any unusual activity is discovered.
- Application logs are rotated hourly and stored for seven days before deletion.
- Reviews of the audit, system and application logs are conducted quarterly in order to detect irregularities, including misuse of computing and application resources.
- SOPs for system administration are in place including an Intrusion Response Plan.
- The DPM application itself allows administrators to monitor application usage and set permissions levels within application. For example, the DPM allows administrators to:
    - Set up data-driven alerts and email notifications within the application.
    - Customize the application to require users to re-enter their password for sensitive/restricted table and record views, or to require a digital signature to confirm their identity when making edits to important record fields.
    - Program the application to restrict records and tables to specific individuals and groups, or with data-driven criteria-based permissions.