Apache Fineract Security Report

This page lists all security vulnerabilities fixed in released version of Apache Fineract. Each vulnerability is given a security impact rating by the Apache security team - please note that this rating may vary from platform to platform.

Fixed in Apache Fineract 1.1.0

CVE-2018-1292: Apache Fineract SQL Injection Vulnerability - Injection via reportName parameter

Critical: Within the 'getReportType' method, a hacker could inject SQL to read/update data for which he doesn't have authorization for by way of the 'reportName' parameter.

Release branch with the **fix** is available at https://github.com/apache/fineract/tree/1.1.0

Acknowledgements: We would like to thank **(627963028@qq.com)** and **Apache Security team** for reporting this issue.

Reported to security team	23 January 2018
Issue public	19 April 2018
Update Released	23 March 2018
Affects	0.4.0-incubating, 0.5.0-incubating, 0.6.0-incubating, 1.0.0

CVE-2018-1291: Apache Fineract SQL Injection Vulnerability - Order by injection via Order Param

Critical: Apache Fineract exposes different REST end points to query domain specific
entities with a Query Parameter 'orderBy' which are appended directly with SQL statements. A hacker/user can inject/draft
the 'orderBy' query parameter by way of the "order" param in such a way to to read/update the data for which he doesn't have authorization.

Release branch with the **fix** is available at https://github.com/apache/fineract/tree/1.1.0

Acknowledgements: We would like to thank **(627963028@qq.com)** and **Apache Security team** for reporting this issue.

Reported to security team	23 January 2018
Issue public	19 April 2018
Update Released	23 March 2018
Affects	0.4.0-incubating, 0.5.0-incubating, 0.6.0-incubating, 1.0.0

CVE-2018-1290: Apache Fineract SQL Injection Vulnerability - Single quotation escape caused by two continuous SQL parameters

Critical: Using a single quotation escape with two continuous SQL parameters can cause a SQL injection. This could be done in Methods like retrieveAudit Entries of AuditsApiResource Class

retrieveCommands of MakercheckersApiResource Class

Release branch with the **fix** is available at https://github.com/apache/fineract/tree/1.1.0

Acknowledgements: We would like to thank **(627963028@qq.com)** and **Apache Security team** for reporting this issue.

Reported to security team	23 January 2018
Issue public	19 April 2018
Update Released	23 March 2018
Affects	0.4.0-incubating, 0.5.0-incubating, 0.6.0-incubating, 1.0.0

CVE-2018-1289: Apache Fineract SQL Injection Vulnerability by orderBy and sortOrder parameters

Critical: Apache Fineract exposes different REST end points to query domain specificentities with a Query Parameter 'orderBy' and 'sortOrder' which

are appended directly with SQL statements. A hacker/user can inject/draft the 'orderBy' and 'sortOrder' query parameter in such a way to read/update the data for which he doesn't have authorization.

Release branch with the **fix** is available at https://github.com/apache/fineract/tree/1.1.0

Acknowledgements: We would like to thank **(627963028@qq.com)** and **Apache Security team** for reporting this issue.

Reported to security team	18 January 2018
Issue public	19 April 2018

Update Released	23 March 2018
Affects	0.4.0-incubating, 0.5.0-incubating, 0.6.0-incubating, 1.0.0

Fixed in Apache Fineract 1.0.0

CVE-2017-5663: Apache Fineract SQL Injection Vulnerability
Critical: An authenticated user with client/loan/center/staff/group read permissions is able to inject malicious SQL into SELECT queries. The 'sqlSearch' parameter on a number of endpoints is not sanitized and appended directly to the query

List of vulnerable endpoints:
- /staff
- /clients
- /loans
- / centers
- /groups

Fix detail: Added logic to sanitize the sqlSearch

Release branch with the **fix** is available at https://github.com/apache/fineract/tree/1.0.0

Acknowledgements: We would like to thank **Alex Ivanov** and **Apache Security team** for reporting this issue.

Reported to security team	02 April 2017
Issue public	13 December 2017
Update Released	01 Jun 2017
Affects	0.4.0-incubating, 0.5.0-incubating, 0.6.0-incubating