Apache Fineract Security Report

This page lists all security vulnerabilities fixed in a released version of Apache Fineract. Each vulnerability is reported via the [http://www.apache.org/security/](http://www.apache.org/security/) process and given a security impact rating by the Apache security team - please note that this rating may vary from platform to platform. If you have identified a security issue, email security AT fineract.apache.org.

Amendment of November 29, 2022: In order to ensure that users are given warning of critical issues, the Apache Fineract project may use its relationship with the independent Mifos Initiative to ensure that users of the Fineract backend and Mifos front end UI are informed of such vulnerabilities and are able to assist in testing and validating patches.

The Apache Fineract project recommends that you secure the platform by not running it directly on the internet. IP filtering and other techniques may be essential for all API ingress. In particular, simply running the solution in default mode, connecting it with a front end UI, is not considered best practice for a production environment of fineract unless additional security layers and practices are added.

### Fixed in Apache Fineract 1.9.0

On 27 February 2024 we announced End of Life of Version 1.8.*. All previous versions may be vulnerable to the following CVEs and we urge our users to upgrade to the latest.

**CVE-2024-23537**

Description: Under certain circumstances, this vulnerability allowed users, without specific permissions, to escalate their privileges to any role, including super user status. This flaw could enable users to gain control over user management.

Fixed by [https://github.com/apache/fineract/pull/3626](https://github.com/apache/fineract/pull/3626)

<table>
<thead>
<tr>
<th>Reported to security team</th>
<th>4 Sept 2023</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed</td>
<td>6 Dec 2023</td>
</tr>
<tr>
<td>Update Released</td>
<td>12 Jan 2024</td>
</tr>
<tr>
<td>Issue public</td>
<td>15 March 2024</td>
</tr>
<tr>
<td>Affects</td>
<td>1.8.4 and earlier releases</td>
</tr>
</tbody>
</table>

Acknowledgements: We thank Yash Sancheti of GH Solutions Consultants for reporting this issue.

**CVE-2024-23538**

Description: Under certain system configurations, the sqlSearch parameter was vulnerable to blind SQL injection attacks, potentially allowing attackers to manipulate database queries.

Fixed by [https://github.com/apache/fineract/pull/3626](https://github.com/apache/fineract/pull/3626)

<table>
<thead>
<tr>
<th>Reported to security team</th>
<th>9 Aug 2023</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed</td>
<td>6 Dec 2023</td>
</tr>
<tr>
<td>Update Released</td>
<td>12 Jan 2024</td>
</tr>
<tr>
<td>Issue public</td>
<td>15 March 2024</td>
</tr>
<tr>
<td>Affects</td>
<td>1.8.4 and earlier releases</td>
</tr>
</tbody>
</table>

Acknowledgements: We thank Majd Alasfar of ProgressSoft for reporting this issue.

**CVE-2024-23539**

Description: Under certain system configurations, the sqlSearch parameter for specific endpoints was vulnerable to SQL injection attacks, potentially allowing attackers to manipulate database queries.

Fixed by [https://github.com/apache/fineract/pull/3621](https://github.com/apache/fineract/pull/3621)

<table>
<thead>
<tr>
<th>Reported to security team</th>
<th>4 Sept 2023</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed</td>
<td>6 Dec 2023</td>
</tr>
</tbody>
</table>
CVE-2023-25195

DESCRIPTION:
Server-Side Request Forgery (SSRF) vulnerability in Apache Software Foundation Apache Fineract.

Authorized users with limited permissions can gain access to server and may be able to use server for any outbound traffic.

This issue affects Apache Fineract: from 1.4 through 1.8.3.

Release branch: The fix is available at 1.8.4 and 1.7.3 patches.

1.8.4 - Apache Fineract
1.7.3 - Apache Fineract

Acknowledgements: We would like to thank Huydoppa from GHTK, for reporting this issue, and the Apache Security team for their assistance. Thank you to Aleks@apache.org for resolving this CVE.

CVE-2023-25196

DESCRIPTION:
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Apache Software Foundation Apache Fineract.

This issue affects Apache Fineract: from 1.4 through 1.8.2.

Release branch: The fix is available at 1.8.4 and 1.7.3 patches.

1.8.4 - Apache Fineract
1.7.3 - Apache Fineract

Acknowledgements: We would like to thank Zhang Baocheng at Leng Jing Qi Cai Security Lab, for reporting this issue, and the Apache Security team for their assistance. Thank you to aleks@apache.org for resolving this CVE.
## FINERACT-1868
- **Paging fix for 1.8.x**
- **RESOLVED**

### CVE-2023-25197
**DESCRIPTION:**
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Apache Software Foundation apache fineract.

This issue affects apache fineract: from 1.4 through 1.8.2.

**Release branch:** The fix is available at 1.8.4 and 1.7.3 patches.

1.8.4 - Apache Fineract  
1.7.3 - Apache Fineract

**Acknowledgements:** We would like to thank Eugene Lim at Cyber Security Group (CSG) Government Technology Agency GOVTECH.sg, for reporting this issue, and the Apache Security team for their assistance. Thank you to @AleksandarVidakovic for resolving this CVE.

---

## FINERACT-1870
- **Run Reports fix for 1.8.x**
- **RESOLVED**

---

### CVE-2022-44635:
**file upload vulnerability**

**DESCRIPTION:** Apache Fineract allowed an authenticated user to perform remote code execution due to a path traversal vulnerability in a file upload component of Apache Fineract, allowing an attacker to run remote code. This issue affects Apache Fineract version 1.8.0 and prior versions. We recommend users to upgrade to 1.8.1.

**Critical:** Apache Fineract fails to protect against a vector of attack.

Under certain conditions of the runtime, a malicious actor could execute code remotely

**Release branch:** The fix is available at 1.8.1 and 1.7.1 patches.

1.8.1 - Apache Fineract
## 1.7.1 - Apache Fineract

**Acknowledgements:** We would like to thank Sapra co-captain of the Super Guesser CTF team & Security researcher at CRED, for reporting this issue, and the [Apache Security team](https://cwe.mitre.org/data/definitions/126.html) for their assistance. We give kudos and karma to @Aleksandar Vidakovic for resolving this CVE.

<table>
<thead>
<tr>
<th>Action</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reported to security team</td>
<td>31 October 2022</td>
</tr>
<tr>
<td>Fixed</td>
<td>22 November 2022</td>
</tr>
<tr>
<td>Update Released</td>
<td>25 November 2022</td>
</tr>
<tr>
<td>Issue public</td>
<td>29 November 2022</td>
</tr>
<tr>
<td>Affects</td>
<td>0.4.0-incubating, 0.5.0-incubating, 0.6.0-incubating, 1.0.0, 1.1.0, 1.2.0, 1.3.0, 1.4.0, 1.5.0, 1.6.0, 1.7.0, 1.8.0</td>
</tr>
</tbody>
</table>

**[REFERENCES]:**

---

### Fixed in Apache Fineract 1.5.0

CVE-2020-17514: Disabled Hostname verification for HTTPS

**[DESCRIPTION]:**

*Critical:* Apache Fineract disables HTTPS hostname verification in `ProcessorHelper` in the `configureClient` method.

Under typical deployments, a man in the middle attack could be successful.

**Release branch:** The fix is available at [https://github.com/apache/fineract/tree/1.5.0](https://github.com/apache/fineract/tree/1.5.0).

**Acknowledgements:** We would like to thank Simon Gerst at [https://github.com/intrigus-lgtm](https://github.com/intrigus-lgtm) for reporting this issue, and the [Apache Security team](https://cwe.mitre.org/data/definitions/126.html) for their assistance.

<table>
<thead>
<tr>
<th>Action</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reported to security team</td>
<td>15 October 2020</td>
</tr>
<tr>
<td>Fixed</td>
<td>19 October 2020</td>
</tr>
<tr>
<td>Update Released</td>
<td>23 May 2021</td>
</tr>
<tr>
<td>Issue public</td>
<td>26 May 2021</td>
</tr>
<tr>
<td>Affects</td>
<td>0.4.0-incubating, 0.5.0-incubating, 0.6.0-incubating, 1.0.0, 1.1.0, 1.2.0, 1.3.0, 1.4.0</td>
</tr>
</tbody>
</table>

**[REFERENCES]:**
[https://issues.apache.org/jira/browse/FINERACT-1211](https://issues.apache.org/jira/browse/FINERACT-1211)

**[ASSIGNINGCNA]:** none

---

### Fixed in Apache Fineract 1.4.0

CVE-2018-20243 : Unencrypted username and password in URL

*Critical:* Passing the password in a URL parameter, instead of POST body, risked exposing this credential e.g. in log files and HTTP intermediaries like proxies.

**Release branch:** The fix is available at [https://github.com/apache/fineract/tree/1.4.0](https://github.com/apache/fineract/tree/1.4.0).

**Acknowledgements:** We would like to thank Abiy Atsbha, <abiyats@gmail.com> for reporting this issue, and the [Apache Security team](https://cwe.mitre.org/data/definitions/126.html) for their assistance.
Additional information see: https://issues.apache.org/jira/browse/FINERACT-726 and https://issues.apache.org/jira/browse/FINERACT-629. Note that Client implementations (front-end UIs) should note this change, and instances in-production should always implement safe techniques for transmission of security credentials.

CVE-2016-4977 : Remote code execution vulnerabilities as a result of CVE in an upstream dependency

Critical: A known vulnerability in spring security upstream dependencies allowed malicious users to trigger remote code execution. Additional details at https://nvd.nist.gov/vuln/detail/CVE-2016-4977

Release branch: The fix is available at https://github.com/apache/fineract/tree/1.3.0

Acknowledgements: We would like to thank Roberto (extranewbugs@gmail.com) for reporting this issue, and the Apache Security team for their assistance.


Important: Two SQL Injection vulnerabilities were reported; the first one in a query on the GroupSummaryCounts table, the second on the m_center data table.

Release branch with the fix is available at https://github.com/apache/fineract/tree/1.3.0

Acknowledgements: We would like to thank Niels Heinen from Google for reporting this issue, and the Apache Security team for their assistance.

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.
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.

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 retrieveAuditEntries 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.

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

Critical: Apache Fineract exposes different REST end points to query domain specific entities 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.

CVE-2018-1280: Apache Fineract SQL Injection Vulnerability by orderBy and sortOrder parameters

Critical: Apache Fineract exposes different REST end points to query domain specific entities 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.

CVE-2018-1279: Apache Fineract SQL Injection Vulnerability by orderBy and sortOrder parameters

Critical: Apache Fineract exposes different REST end points to query domain specific entities 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.

CVE-2018-1278: Apache Fineract SQL Injection Vulnerability by orderBy and sortOrder parameters

Critical: Apache Fineract exposes different REST end points to query domain specific entities 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.

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.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Reported to security team</td>
<td>02 April 2017</td>
</tr>
<tr>
<td>Issue public</td>
<td>13 December 2017</td>
</tr>
<tr>
<td>Update Released</td>
<td>01 June 2017</td>
</tr>
<tr>
<td>Affects</td>
<td>0.4.0-incubating, 0.5.0-incubating, 0.6.0-incubating</td>
</tr>
</tbody>
</table>