INTENTABLE

Powered by KIROBO

Intentable's Smart Transaction technology powered by the Kirobo FCT Platform

FCT Core Security Analysis

by Pessimistic

This report is public

October 2, 2024

Abstract

In this report, we consider the security of smart contracts of Intentable project. Our task is to find and describe security issues in the smart contracts of the platform.

Disclaimer

Summary

In this report, we considered the security of the FCT Core submodule of Intentable smart contracts. We described the audit process in the section below.

The report has designations like C01, M05, L10, N08. The letter represents severity, and the number represents the issue number.

This is a condensed version of the report; a more detailed one can be found at the following links:

The original reports:

- Report #1. The report includes the M04 issue, which was addressed and was relevant to the whole project.
- Report #2. The fixed issues:
    - N02, which was relevant to the current submodule;
    - L04, which was relevant for the whole project.
- Report #3. The report includes:
    - N06, which was relevant to the current submodule;
    - M01, which was addressed and was relevant to the whole project.

The report includes notes with the `commented` status: N01, N02 and N03 (N07, N05 and N06 in the Report #2).

All the tests passed. The code coverage is sufficient.

After the last recheck, which was fully described in Report #3 (see the Codebase update #8) and copied to the Project description, the codebase was updated again. The number of tests and the code coverage increased. We did not find any new issues.

According to our recommendations, the developers split the long function in the **FCT_BatchMultiSig** contract, improving the code readability. However, it is still important to note that the project and its architecture are complex, though we realize that it is difficult or impossible to implement simply.

It is crucial to study the three reports above to get a full picture of the security of smart contracts.

General recommendations

We recommend implementing CI to run tests, calculate code coverage, and analyze code with linters and security tools.

Project overview

Project description

For the audit, we were provided with Intentable project on a private GitHub repository, commit cf31b27dd9e44e016ced8e3060a487e7e1e2d5cc.

It is a condensed version of the report. More detailed information about codebase updates can be found at the following links:

- Report #1;
- Report #2;
- Report #3.

The scope included:

- FCT_Authenticator.sol;
- FCT_Controller.sol;
- FCT_ENS.sol;
- IFCT_Authenticator.sol;
- IFCT_Controller.sol;
- IFCT_Engine.sol;
- IFCT_ENS.sol;
- IFCT_Runner.sol;
- IFCT_RunnerOptional.sol;
- FCT_Auth_FlashLoan.sol;
- FCT_Auth_Vault.sol
- FCT_Auth_SecureStorage.sol.

The documentation for the project included https://kirobo.gitbook.io/fct-developers-guide/.

The total LOC of the audited scope is 686.

All 592 tests passed. The code coverage of the project was 84.64%.

Codebase update #1

For the recheck, we were provided with Intentable project on a private GitHub repository, commit 9ba7299653676b06cadfcbfac2d1f9fff66d333c.

The developers provided the test results and the code coverage. All 630 tests passed, the code coverage of the scope was 95.42%, and the code coverage of the FCT platforms was 92.93%.

Audit process

We started to check the FCT platform around two years ago and created four extensive reports. The developers asked us to split these reports into seven submodules. Each submodule has:

- The last common commit for all reports;
- The same results of the tests and the code coverage for the whole project;
- The individual scope;
- Links to the corresponding previous reports;
- The list of fixed issues, e.g., M01, M04, L03 (see the description in the Summary), etc.;
- The descriptions of unfixed or commented issues that are still actual;
- The findings relevant to the whole project.

Issue descriptions copied from previous reports can have different contract names and lines, as they were checked again and updated due to the last commit in the Project description.

We started auditing the FCT platforms in 2022. During this time, we made three FCT reports and one report for the Smart Wallet part.

Each report is a continuation of the previous one. We made the split in the process to avoid one infinitely extensive report. The chronology of the reports:

- Smart Wallet report - finished on August 15, 2022;
- Report #1 - finished on November 17, 2022;
- Report #2 - finished on July 26, 2023, and last updated on January 16, 2024;
- Report #3 - finished on June 26, 2024.

See the previous reports for a more detailed description of the issues and process. The following rechecks related to a specific module will only appear in the corresponding report.

We made recheck #1 for this scope on June 26-27, 2024. It was the first recheck in this report but not the first one in the entire audit process (see the previous reports). The developers provided the test results and the code coverage, as we could not run them. This update included code refactoring and fixes for adding the new functionality.

Manual analysis

The contracts were completely manually analyzed, their logic was checked. Besides, the results of the automated analysis were manually verified. All the confirmed issues are described below.

Critical issues

Critical issues seriously endanger project security. They can lead to loss of funds or other catastrophic consequences. The contracts should not be deployed before these issues are fixed.

The audit showed no critical issues.

Medium severity issues

Medium severity issues can influence project operation in the current implementation. Bugs, loss of potential income, and other non-critical failures fall into this category, as well as potential problems related to incorrect system management. We highly recommend addressing them.

The audit showed no issues of medium severity.

Low severity issues

Low severity issues do not directly affect project operation. However, they might lead to various problems in future versions of the code. We recommend fixing them or explaining why the team has chosen a particular option.

The audit showed no issues of low severity.

Notes

N01. Replay attack (commented)

FCT can be executed multiple times, even more, than expected in the `repeatsLeft` field of `s_fcts` mapping from the **FCT_Controller** contract.

It can happen since FCT can be purged by anyone and then registered again:

- The `purge` function of the **FCT_Controller** contract deletes `s_fcts[messageHashes[i]]` variable at line 192;
- There is no check that it can be removed only by the owner of FCT. That is why anyone can delete any FCT with a true purgeable flag.

> *<u>Comment from the developers:</u> FCT can be purged only when expire time has passed and it cannot be executed anymore.*

N02. Unsafe delegatecall using (commented)

The using of `delegatecall` is potentially unsafe since the `target` contract may call `selfdestruct`.

In the `fctCall` function of the **RecoveryWallet** contract, `delegatecall` can be called by `ENS_LIBRARY` type target only. And targets of this type can be added through `FCT_ENS.setLocalEns` function by `LOCAL_ENS_ROLE`.

So, this `delegatecall` is protected by the project role. However, if admin's private keys become compromised, any targets can be added.

> *<u>Comment from the developers:</u> In the function `ensToAddress` the second param can be an address or 0, for extra security the user can choose to add the lib address, and so, if the ENS of the lib was changed the FCT will not work.*

> *<u>Pessimistic's comment:</u>*
> *During the rechecks, the **RecoveryWallet** contract was renamed **SmartWallet**.*

N03. **Overpowered roles** (commented)

The project has a lot of roles. They have the following options:

- **FCT_ENS** contract:
  - `ENS_ROLE` can change the address of the **ENS** service, which is used for adding new targets;
  - `LOCAL_ENS_ROLE` can add new targets. This role has an impact on the `delegatecall` in the **RecoveryWallet** contract (see the Unsafe delegatecall using issue);
- **FCT_Controller** contract:
  - `TARGET_ROLE` can add a new engine. This has an impact on the whole system since the wrong address can lead to unpredictable consequences;
  - `ACTUATOR_ROLE` can call the engine through the `fallback` function;
  - `LOCAL_ENS_ROLE` (is not used anymore);
  - `ENS_ROLE` can set the address of the **FCT_ENS** contract.

Thus, if the admin's private keys are compromised, there may be scenarios that could lead to undesirable consequences for the project and its users.

> *Comment from the developers:* *Now we are using the same key for all, but in production we plan to add multiSig for that.*

> *Pessimistic's comment:*
> *During the rechecks, the **RecoveryWallet** contract was renamed **SmartWallet**.*

This analysis was performed by Pessimistic:

Daria Korepanova, Senior Security Engineer
Yhtyyar Sahatov, Security Engineer
Evgeny Bokarev, Junior Security Engineer
Konstantin Zherebtsov, Business Development Lead
Irina Vikhareva, Project Manager
Alexander Seleznev, CEO

October 2, 2024