Talofa Corporation
Smart Contract
Audit Report

contact@movebit.xyz

https://twitter.com/movebit_

05/18/2023

Talofa Corporation Smart Contract Audit Report

1 Executive Summary

1.1 Project Information

Description	Run Legends game from Talofa is a fitness battle game where your movement unleashes attacks and special skills.
Type	GameFi
Auditors	MoveBit
Timeline	May 15, 2023 – May 18, 2023
Languages	Move
Platform	Sui
Methods	Architecture Review, Unit Testing, Manual Review
Source Code	git@github.com:MystenLabs/talofa.git
Commits	de93f70443bd31170e22c2fe14aae603c06f1b90

1.2 Files in Scope

The following are the SHA1 hashes of the last reviewed files.

ID	Files	SHA-1 Hash
RLGD	run_legends_v0.3/sources/run_legends.move	59f350e2593b53b73c6a131d4516505f6e96424e

GEAR	run_legends_v0.3/sources/gear.move	b63725163c8958b833a08c3afe500ebe62d25748

1.3 Issue Statistic

Item	Count	Fixed	Acknowledged
Total	3		3
Informational			
Minor	2		2
Medium			
Major	1		1
Critical			

1.4 MoveBit Audit BreakDown

MoveBit aims to assess repositories for security-related issues, code quality, and compliance with specifications and best practices. Possible issues our team looked for included (but are not limited to):

- Transaction-ordering dependence
- Timestamp dependence
- Integer overflow/underflow by bit operations
- Number of rounding errors
- Denial of service / logical oversights
- Access control
- Centralization of power
- Business logic contradicting the specification
- Code clones, functionality duplication
- Gas usage
- Arbitrary token minting

- Unchecked CALL Return Values
- The flow of capability
- Witness Type

1.5 Methodology

The security team adopted the "**Testing and Automated Analysis**", "**Code Review**" and "**Formal Verification**" strategy to perform a complete security test on the code in a way that is closest to the real attack. The main entrance and scope of security testing are stated in the conventions in the "Audit Objective", which can expand to contexts beyond the scope according to the actual testing needs. The main types of this security audit include:

(1) Testing and Automated Analysis

Items to check: state consistency / failure rollback / unit testing / value overflows / parameter verification / unhandled errors / boundary checking / coding specifications.

(2) Code Review

The code scope is illustrated in section **1.2**.

(3) Formal Verification

Perform formal verification for key functions with the Move Prover.

(4) Audit Process

- Carry out relevant security tests on the testnet or the mainnet;
- If there are any questions during the audit process, communicate with the code owner in time. The code owners should actively cooperate (this might include providing the latest stable source code, relevant deployment scripts or methods, transaction signature scripts, exchange docking schemes, etc.);
- The necessary information during the audit process will be well documented for both the audit team and the code owner in a timely manner.

2 Summary

This report has been commissioned by **Talofa Corporation** to identify any potential issues and vulnerabilities in the source code of the **Run Legend** smart contract, as well as any contract

dependencies that were not part of an officially recognized library. In this audit, we have utilized various techniques, including manual code review and static analysis, to identify potential vulnerabilities and security issues.

During the audit, we identified **3** issues of varying severity, listed below.

ID	Title	Severity	Status
GEAR-01	Missing Permission Verification	Major	Acknowledged
GEAR-02	Missing Emit Event	Minor	Acknowledged
GEAR-03	Reliance on Third-party Library Files	Minor	Acknowledged

3 Participant Process

Here are the relevant actors with their respective abilities within the **Run Legend** Smart Contract :

Admin

- Admin can mint `Gear` through `admin_mint()`.
- Admin can update the `Gear` through `update_gear_description()`, `update_gear_level()`, `update_gear_audio()`, `update_gear_visual()`, `update_gear_img()`, `add_skill()`, `update_skill()`, `update_skill_effect()`, `update_skill_interval()`, `update_skill_max_duration()`, `update_skill_cooldown()`.
- Admin can lock `Gear` updates and export Gear to a kiosk under a non-custodial wallet through `export_gear_to_kiosk()`.
- Admin can create a TransferToken between custodial and external wallet for players through `admin_create_transfer_token()`.
- Admin can create a `kiosk` for a given address through `create_kiosk_for_ncw()`.
- Admin can unlock `Gear` updates for gears that reside in a custodial wallet through `unlock_gear_in_cw()`.
- Admin can issue a `UpdateCap` for unlocking `Gear` updates in the custodial wallet through `admin_issue_update_cap_for_cw()`.

Player

- Players can withdraw a `Gear` from their kiosk through `import_gear_to_cw()`.

4 Findings

GEAR-01 Missing Permission Verification

Severity: Major

Status: Acknowledged
Code Location: run_legends_v0.3/sources/gear.move#L223-L367.
Descriptions: These update functions do not check caller permissions, and the `Gear` owner can change the parameter configuration of `Gear` and `Skill`.

Suggestion: It is recommended to confirm if it aligns with the design.

Resolution: The client decided not to fix it because the gears can only be updated through the in-game custodial wallet (according to the "exported" function) and Talofa is the only owner of the custodial wallet.

GEAR-02 Missing Emit Event

Severity: Minor

Status: Acknowledged
Code Location: run_legends_v0.3/sources/gear.movee#L223-L367.
Descriptions: The smart contract lacks appropriate events for monitoring sensitive operations, which could make it difficult to track important actions or detect potential issues.

Suggestion: It is recommended to emit an event for these update functions.

Resolution: The client decided not to fix it because the program was designed to do so.

GEAR-03 Reliance on Third-party Library Files

Severity: Minor

Status: Acknowledged
Code Location: run_legends_v0.3/sources/gear.move.

Descriptions: During the audit, it was observed that the contract incorporates a substantial number of external libraries in https://github.com/Origin-Byte/nft-protocol. These libraries, although not included in the scope of this audit, are essential for the proper functioning of the contract. It is assumed that you have already assessed and verified the security and reliability of these dependencies.

Suggestion: Given that the audit scope does not cover the external libraries used in the contract, it is crucial to ensure that a thorough review and assessment of these libraries have been conducted by your team or a trusted third party. Additionally, it is recommended to regularly monitor and update these dependencies to mitigate any potential risks arising from vulnerabilities or compatibility issues in the future.

Resolution: The client confirmed the issue and replied to the Third-party library already went through a security audit.

Appendix 1

Issue Level

- **Informational** issues are often recommendations to improve the style of the code or to optimize code that does not affect the overall functionality.
- **Minor** issues are general suggestions relevant to best practices and readability. They don't post any direct risk. Developers are encouraged to fix them.
- **Medium** issues are non-exploitable problems and not security vulnerabilities. They should be fixed unless there is a specific reason not to.
- **Major** issues are security vulnerabilities. They put a portion of users' sensitive information at risk, and often are not directly exploitable. All major issues should be fixed.
- **Critical** issues are directly exploitable security vulnerabilities. They put users' sensitive information at risk. All critical issues should be fixed.

Issue Status

- **Fixed:** The issue has been resolved.
- **Partially Fixed**: The issue has been partially resolved.
- **Acknowledged:** The issue has been acknowledged by the code owner, and the code owner

confirms it's as designed, and decides to keep it.

Appendix 2

Disclaimer

This report is based on the scope of materials and documents provided, with a limited review at the time provided. Results may not be complete and do not include all vulnerabilities. The review and this report are provided on an as-is, where-is, and as-available basis. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your own risk. A report does not imply an endorsement of any particular project or team, nor does it guarantee its security. These reports should not be relied upon in any way by any third party, including for the purpose of making any decision to buy or sell products, services, or any other assets. TO THE FULLEST EXTENT PERMITTED BY LAW, WE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, IN CONNECTION WITH THIS REPORT, ITS CONTENT, RELATED SERVICES AND PRODUCTS, AND YOUR USE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NOT INFRINGEMENT.