SharkTeam

No.20221216002C

Smart Contract Audit Report

Infamous NFT

Dec. 16th, 2022

Copyright

1. Overview

SharkTeam recently received the requirements for Infamous NFT smart contracts audit. In this audit, the SharkTeam security experts communicate with Infamous NFT team to conduct smart contract security audit under controllable operation, so as to avoid any risk in the audit process as far as possible.

Project Overview :

Project Name	Infamous NFT
Description	NFT, GameFi
Language	Move
Codebase	https://github.com/MatrixLabsTech/infamous-nft-contract
Commit	06a0721d023d6d1f75d7baac73bab84b3bda248d

Audit method :

SharkTeam security experts conducted a detailed manual audit of the smart contracts line-by-line. From the four dimensions of high-level language, virtual machine, blockchain, and business logic, much more audit items of smart contracts have been comprehensively audited. Especially for common high-risk vulnerabilities in Move language, smart contracts and related businesses including DeFi, GameFi and NFT, we have conducted in-depth audits.

Audit Items:

For the Move smart contract, SharkTeam's audit items cover four layers: language, virtual machine, blockchain, and business, and four levels of high risk, medium risk, low risk, and information. Some of the common high-risk items (not all vulnerabilities) are as follows:

- Resource and Function Visibility
- Module and Resource Initialization
- Token Minting and Burning
- Authority and Access Control
- Centralization of Power
- Function Logic Vulnerability
- Flashloan and Price Manipulation
- DAO Proposal Attack
- Contract Upgrade Issues
- Randomness and Revert Attack
- Insufficient Randomness
- Integer Overflow/Underflow
- Divide/Multiply and Integer Precision
- Unchecked/Unused Return Values
- Blockchain Timestamp
- Transaction Order Dependency and Front Running
- Denial of Service (DoS)

Audit Scope :

Contract Files	MD5
contracts/source/infamous_common.move	8d7a0c48a48e61bf6502a6a1e0c11f5b
contracts/source/infamous_manager_cap.move.move	9b0db33d1649ea252015e3f88a185340
contracts/source/infamous_backend_auth.move	a1ad6ba88b42ef9ae3a8d9a7c790f3a1
contracts/source/infamous_accessory_nft.move	ff661274b38e5fb88c5f0579602dd30c
contracts/source/infamous_weapon_nft.move	45435c40b05233892d1771b0c352a018
contracts/source/infamous_properties_url_encode_map.move	3bf844885478c31f00ad484ff53caa66
contracts/source/infamous_link_status.move	1393ba9631a0728df1dbddc1ec299e26
contracts/source/infamous_nft.move	5184d305d39eba09de2b1467a9504937
contracts/source/infamous_backend_token_accessory_open_box.move	edf05484515433d2005c84a2e1c74137
contracts/source/infamous_backend_token_weapon_open_box.move	14c31b1236708a2709f4be790d1e691e
contracts/source/infamous_backend_	765bd1b54e7e701bedb60fe68340f80f

open_box.move	
contracts/source/infamous_lock.move	b6aec35a129ab221c7b6e115b7e2f8d9
contracts/source/infamous_weapon_wear.move	cdbf6bffff25005208fdee7883a19b85
contracts/source/infamous_change_accesory.move	1ff39b44877b7cda6308e60a0c5501b3
contracts/source/infamous_upgrade_level.move	dcd638d1c9630e4dafb8523bd776f350

Audit results :

Infamous NFT smart contract audit results: **Pass**.

2. Findings

2.1 Summary

Vulnerability list :

ID	Item	Severity	Category	Status
1	Blockchain Timestamp	Info	Blockchain	Unresolved
2	Centralization of Power	Info	Business	Unresolved
3	Code Specification	Info	Language	Resolved

2.2 Detailed Results

2.2.1 Blockchain Timestamp [Info]

Description:

While upgrading the Infamous NFT, it is necessary to calculate the available locked time of the Infamous NFT, which depends on the blockchain timestamp. Considering that it is extremely difficult to exploit and profit from this vulnerability, and the repair solution is relatively complicated, it is not necessary to repair it.

Recommendation:

(1) Use off-chain third-party timestamp oracles, but additional fees are required;

(2) Use block.number instead of block.timestamp, but not accurate enough.

2.2.2 Centralization of Power [Info]

Description:

There are several key business functions in the contracts, such as the open_box function, which can only be called by administrator accounts, including Infamous account and delegated manager accounts, especially the Infamous account, which can delegate management rights to other accounts.

Once these administrative accounts are compromised, the entire project is no longer safe. Therefore, it is necessary to ensure that the administrator account is safe and trustworthy.

Recommendation:

(1) Properly manage Infamous accounts to avoid leakage of private keys, account theft, etc.

(2) As far as possible to ensure that the delegated manager account is credible.

Appendix A: Vulnerability Severity Classification

The nature of vulnerabilities is unintentional and unexpected security flaws or risks, which can be divided into four threat levels: High, Medium, Low and Info. The classification is mainly based on the impact, likelihood of utilization and other factors.

The impact is defined mainly according to the three dimensions of confidentiality, integrity and availability;

The likelihood of utilization is defined mainly according to three dimensions: attack vector, attack complexity and authentication.

Impact / Likelihood	critical	high	medium	low
low	High	High	Medium	Low
medium	High	Medium	Low	Low
high	Medium	Low	Low	Info
Ex-high	Low	Low	Info	Info

Disclaimer

SharkTeam has tried the best to ensure the accuracy and reliability of the content when writing this report, but SharkTeam will not be responsible for the loss and damage caused by the omission, inaccuracy or error in this report. The safety audit analysis and other contents of this report are based on the materials provided by the project team. This audit only focuses on the audit items provided in this report, and other unknown security vulnerabilities are not within the scope of this audit. SharkTeam cannot determine the security status of facts that appear or exist after the report. SharkTeam is not responsible for the background or other circumstances of the project.

The content, services and any resources involved in this report cannot be used as the basis for any form of investment, taxation, law, and supervision, and there is no relevant responsibility.

About SharkTeam

SharkTeam, a leading blockchain security service team, offers smart contract audit services for developers. To satisfy the demands of different clients, thesmart contract audit services provide both manual auditing and automated auditing.

We implement almost 200 auditing contents that cover four aspects: high-level language layer, virtual machine layer, blockchain layer, and business logiclayer, ensuring that smart contracts are completely guaranteed and Safe.

SharkTeam

In Math，We Trust!

https://sharkteam.org

https://t.me/sharkteamorg

https://twitter.com/sharkteamorg