STAYSAFU AUDIT

July 31ST, 2022

Faded and Famous NFT

TABLE OF CONTENTS

AUDIT SUMMARY

This report was written for Faded and Famous NFT in order to find flaws and vulnerabilities in the Faded and Famous NFT project's source code, as well as any contract dependencies that weren't part of an officially recognized library.

A comprehensive examination has been performed, utilizing Static Analysis, Manual Review, and Faded and Famous NFT Deployment techniques. The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors
- Assessing the codebase to ensure compliance with current best practices and industry standards
- Ensuring contract logic meets the specifications and intentions of the client
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders
- Through line-by-line manual review of the entire codebase by industry expert

AUDIT OVERVIEW

PROJECT SUMMARY

Project name	Faded and Famous NFT
Description	Ethereum NFT project with Stackable Mutations & Crosschain Cryptocurrency [Faded and Famous: Team]
Platform	Ethereum
Language	Solidity
Codebase	MD5 Sum | File Name 2bad7b69331ace1e0cc7e576581b81f3 contract.sol

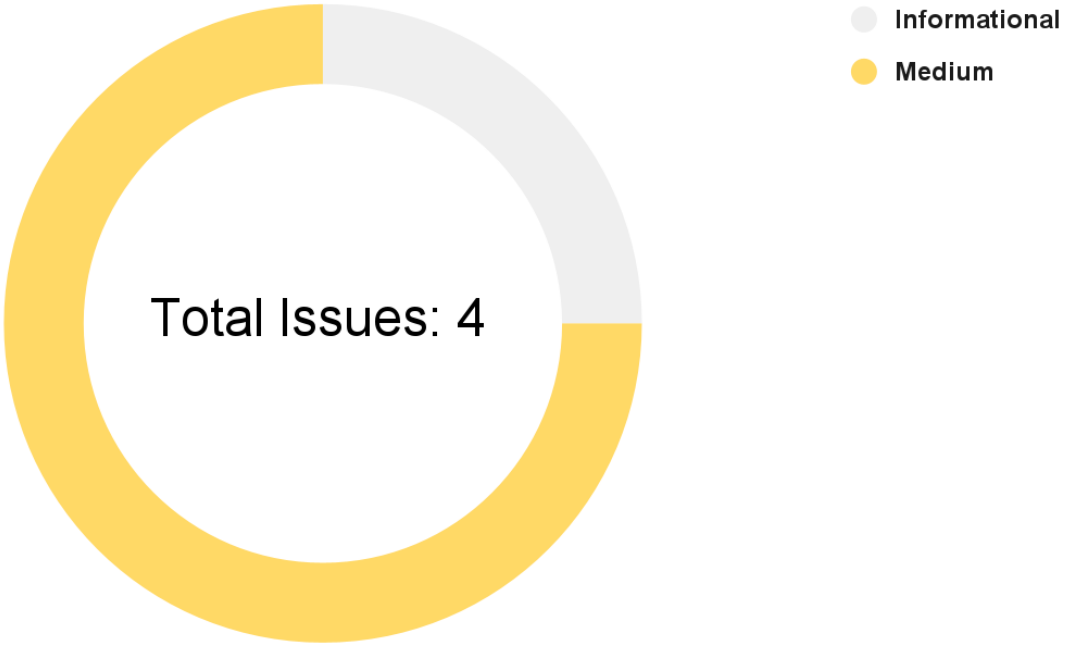
FINDINGS SUMMARY

Vulnerability	Total
Critical	0
Major	0
Medium	3
Minor	0
Informational	1

EXECUTIVE SUMMARY

There have been no major or critical issues related to the codebase and all findings listed here range from informational to medium. The medium security issues are the dependence on a decentralized exchange platform, centralization of privileges, and missing threshold checks.

AUDIT FINDINGS



Code	Title	Severity
CENT-1	Centralization of major privileges	Medium
EXT-1	External protocol dependencies	Medium
MATH-1	Divide before multiply	Medium
MSG-1	Lack of NatSpec Comments	Informational

CENT-1 | Centralization of major privileges | FIXED

Description

The onlyOwner modifier in the smart contract(s) give major privileges over them (whitelist, start sale)*. This can be a problem, in the case of a hack, an attacker who has taken possession of this privileged account could damage the project and the investors.
*This list is not exhaustive but presents the most sensitive points

Recommendation

We recommend at least to use a multi-sig wallet as the owner address, and at best to establish a community governance protocol to avoid such centralization.
See: https://solidity-by-example.org /app/multi-sig-wallet/

EXT-1 | Dependence to an external protocol

Description

The contract serves as an underlying entity to interact with third party OpenSea protocols. The scope of the audit would treat this third party entity as black box and assume it is fully functional. However in the real world, third parties may be compromised and may have led to assets lost or stolen.

Recommendation

We encourage the team to constantly monitor the security level of the entire OpenSea project, as the security of the token is highly dependent on the security of the decentralized exchange platform.

MATH-1 | Divide before multiply

Description

Certain operations in Faded and Fresh NFT's contract perform both multiplication and division operations on a variable, some instances of which perform division before multiplication. This is not best practice and should be avoided where possible, as it could lead to rounding errors. Where these division first operations have been identified are listed below.

- -require -> Line 148
- -require -> Line 151
- -require -> Line 154
- -require -> Line 157
- -require -> Line 160
- -require -> Line 163
- -require -> Line 166
- -require -> Line 169
- -require -> Line 172
- -require -> Line 184
- -require -> Line 187
- -require -> Line 193
- -require -> Line 196
- -require -> Line 199

Recommendation

We recommend these found operations be modified to perform multiplication first and then division, in most cases simply swapping the division and multiplication operations should be sufficient however any changes made should be tested.

MSG-1 | Limited NatSpec comments | FIXED

Description

Throughout Faded and Famous NFT's contracts many functions remain uncommented. This can make understanding the code's functionality difficult for developers and users (if the code is open source) thus reducing maintainability.

Recommendation

We recommend using NatSpec standard comments throughout all contracts.

See: https://docs.soliditylang.org/en/v0.5.17/style-guide.html?highlight=natspec%23natspec

DISCLAIMER

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to the Company in connection with the Agreement.

This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement.

This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes without StaySAFU's prior written consent.This report is not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team or project that contracts StaySAFU to perform a security assessment.

This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with

any particular project.

This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk.

StaySAFU's position is that each company and individual are responsible for their own due diligence and continuous security. StaySAFU's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or fun.