hack·a·chain

SECURITY AUDIT REPORT

in favor of META FIGHTER

Summary

This report has been prepared for MetaFighters in the source code of the project as well as in project dependencies that are not part of an officially recognized library. The audit has been conducted by combining static and dynamic code analysis with a manual review of the source code by Hack-a-Chain's research team.

The audit process analyses:

1) Adherence to widely recognized best practices and industry standards;
2) Vulnerability to most common attack vectors;
3) Thorough line-by-line review of the code base;
4) Ensuring that contract logic meets the specifications of the project's whitepaper.

The security audit result is composed of different findings, whose vulnerabilities are classified from critical to informational, according to the following impact versus likelihood matrix:

Impact	High	Medium	Low
High	Critical	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low / Informational

Likelihood

After presenting the findings to the client, they are granted a 7 days period to fix the vulnerabilities. This report will specify all vulnerabilities found and whether they were fixed by the team.

Overview

Project Summary

Project Name	Meta Fighter
Description	Marketplace contract used to buy and sell NFTs from the game using the project's native currency. SpotTokenManagement contract used to manage in game balance
Platform	BSC (Binance Smart Chain protocol, EVM)
Language	Solidity
Codebase	https://gitlab.com/fruktorum/backend/meta-fighter/contracts/test
Commit	cf1e003c09164057fc6d0de6a816649ebb77db2a

Audit Summary

First delivery date	01/12/2023
Final delivery date	02/07/2023
Audit Methodology	Manual review combined with static/dynamic analysis

Audit Scope

ID	File	SHA256 Checksum
MKT	Marketplace.sol	dc9227b044ba404cffc4e5e277cfd28cb12aac257b9561793f5d39b4d27f9b8b
STM	SpotTokenManagement.sol	32d945f76d2346746b3935e7eb27dda408f197e66fd69704f8ede384befaa01a

Findings

ID	Title	Category	Severity	Status
MKT-1	Unutilized global variables	Gas optimization and/or incomplete logic	Informational	Alleviated

MKT-2	Inconsistent variable naming	Maintainability	Informational	Alleviated
MKT-3	Inconsistent usage of safeTransfer	Consistency	Informational	Alleviated

MKT-1 - Unutilized global variables

Category	Severity	Location	Status
Gas optimization and/or incomplete logic	Informational	Marketplace.sol:18	Alleviated

Description

The contract contains a global variable _tradingFee and _creatorFee, of type uint256 which were never utilized.

Apparently the variables would be used to implement a fee charging logic on top of the marketplace.

Recommendation

We advise the removal of the variables or the implementation of fee logic.

Alleviation

Team implemented tradingFee logic, making it possible for Admin to set the fee that is going to be deducted from every payment made to sellers.

MKT-2 - Inconsistent variable naming

Category	Severity	Location	Status
Maintainability	Informational	Marketplace.sol: 18, 19, 20, 21, 32, 97	Alleviated

Description

We have identified 2 types of inconsistency in variable naming throughout the contract. Even though variable naming does not create any immediate security threat, it makes the code harder to read which might contribute to the future introduction of bugs.

Global variables _tradingFee, _creatorFee and _tokenIdsOfSeller all start with an underscore (_). This standard is commonly used in solidity to name function parameters, specially when they conflict with the name of a global variable in the contract. Using the underscore to name global variables may lead to confusion and to these variables eventually being removed from scope inside functions that have parameters with clashing names.

Throughout the contract, the user action of putting an NFT up for sale is referred to as an order (orderCreated event, createOrder and cancelOrder functions). However, in marketplace terminology, putting an asset up for sale is usually regarded as a listing, whilst an order is used to refer to a purchase being made. This name may confuse developers, auditors and advanced users.

Recommendation

We advise:

(1) The alteration of global variable names starting with an underscore (_) to remove the underscore;

(2) Changing every use of the name “order” for “listing” or other more proper name.

Alleviation

The team implemented the suggested changes to make the code more readable.

MKT-3 - Inconsistent usage of safeTransfer

Category	Severity	Location	Status
Consistency	Informational	Marketplace.sol:106	Alleviated

Description

All NFT transferring operations in the contract utilize the safeTransferFrom method. However, in the cancelOrder function, the normal transferFrom operation is used with no apparent reason.

In the current setup it is unclear to an external auditor or developer whether there is a special reason for such or if it is a simple inconsistency found in the code.

Recommendation

We advise the consistent use of safeTransferFrom or transferFrom in all NFT operations, unless a very specific reason for an exception is needed, in which case the choice should be thoroughly documented on the function that escapes the norm.

Alleviation

The team changed the code base to always utilize safeTransferFrom.

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 you ("Customer" or 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, nor may copies be delivered to any other person other than the Company, without Hack-a-Chain's prior written consent in each instance.

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 Hack-a-Chain 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 intended 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. Hack-a-Chain's position is that each company and individual are responsible for their own due diligence and continuous security.

Hack-a-Chain'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 functionality of the technology we agree to analyze.

The assessment services provided by Hack-a-Chain are subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS,OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED “AS IS” AND “AS AVAILABLE” AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, HACK-A-CHAIN HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, HACK-A-CHAIN SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, HACK-A-CHAIN MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER’S OR ANY OTHER PERSON’S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE. WITHOUT LIMITATION TO THE FOREGOING, HACK-A-CHAIN PROVIDES NO WARRANTY OR UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER’S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED. WITHOUT LIMITING THE FOREGOING, NEITHER HACK-A-CHAIN NOR ANY OF HACK-A-CHAIN’S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. HACK-A-CHAIN WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER’S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED “AS IS” AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT HACK-A-CHAIN’S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST HACK-A-CHAIN WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF HACK-A-CHAIN CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST HACK-A-CHAIN WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

SECURITY AUDIT CERTIFICATE

Deliq Finance

We, Hack-a-Chain, Blockchain Specialist Software Development and Audit Company, in this act represented by our Chief Technology Officer, João Antônio Schmidt da Veiga, grant this **Security Audit Certificate** in favor of **Metafigthers**, recognizing that they have passed throw the security audit process and corrected all the issues that have been found in the following smart contract:

1. **Marketplace contract**
   Deployment address: 0x39C44BDCA65181B3Eb4743e1D069D19387e77fb4
2. **SpotTokenManagement contract**
   Deployment address: 0xE44ca781ce33f084F6F2B6c92aDFF8fd708266C3

The full security audit report and it's disclaimer can be found in the following link:

https://github.com/hack-a-chain/security-audits

Devoted to enhancing security in the Blockchain Ecosystem and to provide the best

quality service for our clients and the community, we sign this Certificate:

João Antônio Schmidt da Veiga
Chief Technology Officer