HACKEN

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

Customer: Game of Silks
Date: April 26th, 2022

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Document

Name	Smart Contract Code Review and Security Analysis Report for Game of Silks.
Approved By	Evgeniy Bezuglyi | SC Department Head at Hacken OU
Type	ERC721 Token
Platform	EVM
Language	Solidity
Methods	Architecture Review, Functional Testing, Computer-Aided Verification, Manual Review
Website	https://www.silks.io/
Timeline	19.04.2022 - 26.04.2022
Changelog	20.04.2022 - Initial Review

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Table of contents

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Introduction

Hacken OÜ (Consultant) was contracted by Silks (Customer) to conduct a Smart Contract Code Review and Security Analysis. This report presents the findings of the security assessment of the Customer's smart contracts.

Scope

The scope of the project is smart contracts in the repository:

Initial review scope
Deployed contract:
https://rinkeby.etherscan.io/address/0x2c6479ffd9d1ab1fce79e894a690238d95d145cd#code
Technical Documentation: No
JS tests: No
Contracts:
File: ./Silks.sol
File: ./external/ERC721A.sol

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
High	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they cannot lead to assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that cannot have a significant impact on execution

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Executive Summary

The score measurements details can be found in the corresponding section of the methodology.

Documentation quality

The Customer provided Whitepaper. The total Documentation Quality score is **5** out of **10**.

Code quality

The total CodeQuality score is **3** out of **10**. No unit tests were provided, used functions exist, some code-style guide violations.

Architecture quality

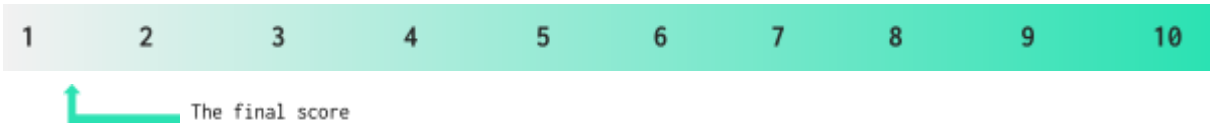
The architecture quality score is **5** out of **10**. The development environment was not provided.

Security score

As a result of the audit, security engineers found **2 high, 1 medium and 1 low** severity issue. The security score is **0** out of **10**.

Summary

According to the assessment, the Customer's smart contract has the following score: **1.3**



Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Checked Items

We have audited provided smart contracts for commonly known and more specific vulnerabilities. Here are some of the items that are considered:

Item	Type	Description	Status
Default Visibility	SWC-100 SWC-108	Functions and state variables visibility should be set explicitly. Visibility levels should be specified consciously.	Passed
Integer Overflow and Underflow	SWC-101	If unchecked math is used, all math operations should be safe from overflows and underflows.	Not Relevant
Outdated Compiler Version	SWC-102	It is recommended to use a recent version of the Solidity compiler.	Failed
Floating Pragma	SWC-103	Contracts should be deployed with the same compiler version and flags that they have been tested thoroughly.	Failed
Unchecked Call Return Value	SWC-104	The return value of a message call should be checked.	Not Relevant
Access Control & Authorization	CWE-284	Ownership takeover should not be possible. All crucial functions should be protected. Users could not affect data that belongs to other users.	Passed
SELFDESTRUCT Instruction	SWC-106	The contract should not be destroyed until it has funds belonging to users.	Not Relevant
Check-Effect-Interaction	SWC-107	Check-Effect-Interaction pattern should be followed if the code performs ANY external call.	Not Relevant
Uninitialized Storage Pointer	SWC-109	Storage type should be set explicitly if the compiler version is < 0.5.0.	Not Relevant
Assert Violation	SWC-110	Properly functioning code should never reach a failing assert statement.	Not Relevant
Deprecated Solidity Functions	SWC-111	Deprecated built-in functions should never be used.	Not Relevant
Delegatecall to Untrusted Callee	SWC-112	Delegatecalls should only be allowed to trusted addresses.	Not Relevant
DoS (Denial of Service)	SWC-113 SWC-128	Execution of the code should never be blocked by a specific contract state unless it is required.	Passed

Race Conditions	SWC-114	Race Conditions and Transactions Order Dependency should not be possible.	Passed
Authorization through tx.origin	SWC-115	tx.origin should not be used for authorization.	Passed
Block values as a proxy for time	SWC-116	Block numbers should not be used for time calculations.	Passed
Signature Unique Id	SWC-117 SWC-121 SWC-122	Signed messages should always have a unique id. A transaction hash should not be used as a unique id.	Passed
Shadowing State Variable	SWC-119	State variables should not be shadowed.	Passed
Weak Sources of Randomness	SWC-120	Random values should never be generated from Chain Attributes.	Passed
Incorrect Inheritance Order	SWC-125	When inheriting multiple contracts, especially if they have identical functions, a developer should carefully specify inheritance in the correct order.	Passed
Calls Only to Trusted Addresses	EEA-Level-2 SWC-126	All external calls should be performed only to trusted addresses.	Passed
Presence of unused variables	SWC-131	The code should not contain unused variables if this is not justified by design.	Failed
EIP standards violation	EIP	EIP standards should not be violated.	Not Relevant
Assets integrity	**Custom**	Funds are protected and cannot be withdrawn without proper permissions.	Passed
User Balances manipulation	**Custom**	Contract owners or any other third party should not be able to access funds belonging to users.	Passed
Data Consistency	**Custom**	Smart contract data should be consistent all over the data flow.	Passed
Flashloan Attack	**Custom**	When working with exchange rates, they should be received from a trusted source and not be vulnerable to short-term rate changes that can be achieved by using flash loans. Oracles should be used.	Not Relevant
Token Supply manipulation	**Custom**	Tokens can be minted only according to rules specified in a whitepaper or any other documentation provided by the customer.	Not Relevant

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Gas Limit and Loops	**Custom**	Transaction execution costs should not depend dramatically on the amount of data stored on the contract. There should not be any cases when execution fails due to the block gas limit.	Passed
Style guide violation	**Custom**	Style guides and best practices should be followed.	Failed
Requirements Compliance	**Custom**	The code should be compliant with the requirements provided by the Customer.	Passed
Repository Consistency	**Custom**	The repository should contain a configured development environment with a comprehensive description of how to compile, build and deploy the code.	Failed
Tests Coverage	**Custom**	The code should be covered with unit tests. Tests coverage should be 100%, with both negative and positive cases covered. Usage of contracts by multiple users should be tested.	Failed

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

System Overview

ERC721A is a NFT contract:

- ERC721A – is a contract based on ERC-721 but using a custom approach of storing the ownership information and tokens minting/transferring algorithms.
  It has the following attributes:
  - Name: Name of the token
  - Symbol: Symbol of the token
  - maxBatchSize: how many tokens can be minted per single transaction
- Silks – is a contract derived from ERC721A with the facility participating in the public sale.
  It has the following attributes:
  - Name: Name of the token
  - Symbol: Symbol of the token
  - baseTokenUri: base URI for tokens
  - numericValues - basic parameters for sale/presale

Privileged roles

- The owner of the contract has the ability to mint tokens.
- The owner of the contract can pause/unpause the contract. If the contract is on pause, sale and pre-sale facilities are blocked.
- The payees of the contract can withdraw their part of earnings by using the proportion provided in the share parameters at the moment of contract deployment.

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Findings

Critical

No critical severity issues were found.

High

1. **Wrong indexes.**

   Token indexes are inconsistent. ‘tokenByIndex’function returns zero if zero is passed as a parameter.
   ‘ownerOf’ function will fail if zero is passed as a parameter.
   ‘tokenOfOwnerByIndex’ function will return one, not zero.
   Such an approach adds additional complexity to the smart contract code and the code of systems that will use those contracts.
   Contracts:ERC721A.sol

   Function: tokenByIndex, tokenOfOwnerByIdex, ownershipOf.

   Recommendation: Use indexes starting from 0 to reduce code complexity.

   Status: New

2. **Potential DoS.**

   The function iterates over all existing tokens.

   Gas consumption can differ a lot between different transactions. Possible DoS if the number of tokens is large enough.

   Contracts:ERC721A.sol

   Function: tokenOfOwnerByIndex

   Recommendation: do not iterate over all tokens.

   Status: New

Medium

1. **Wrong pre-sale detection algorithm.**

   If the pre-sale period is active, then the public sale time has come, and pre-sale period should end automatically. However, it will not.
   Therefore all users who did not have time to buy a token during the pre-sale period are still eligible to buy the token. The problem is “&&” operator has a higher priority than “||” operator.

   Contracts:Silks.sol

   Function: isPreSaleActive

   Recommendation:
   Circle braces should be used to manage priority order. Next code should work:(_preSaleTime == 0 || _preSaleTime < block.timestamp) && (block.timestamp < _publicSaleTime);

Status: New

Low

1. Unused functions

It contains unused functions.

Contracts:ERC721A.sol

Functions: _setOwnersExplicit, _numberMinted

Recommendation: remove unused functions.

Status: New

Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

Disclaimers

Hacken Disclaimer

The smart contracts given for audit have been analyzed by the best industry practices at the date of this report, with cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report (Source Code); the Source Code compilation, deployment, and functionality (performing the intended functions).

The audit makes no statements or warranties on the security of the code. It also cannot be considered a sufficient assessment regarding the utility and safety of the code, bug-free status, or any other contract statements. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only – we recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts.

Technical Disclaimer

Smart contracts are deployed and executed on a blockchain platform. The platform, its programming language, and other software related to the smart contract can have vulnerabilities that can lead to hacks. Thus, the audit cannot guarantee the explicit security of the audited smart contracts.