Swiss Shield

SMART CONTRACT AUDIT OF

KRABOTS

July 19, 2022

@SwissShieldLabs

Project Overview

Krabots is the auto-combat robot fighting game. You play as Krasers to collect NFT robot parts, assemble and upgrade your ultimate Krabot, and defeat your opponent to move on in the Krabots tournament.

Besides the unpredictable physics-based battle, Krabots has a player-driven economy where everyone can buy, sell, and trade with other players at an NFT Marketplace.

Krabot is one of seven worlds in the Iron Sail project. With the cooperation of Hikergames and Whydah, Krabots wants to bring players simplicity but still extremely captivating.

The mission is to build a large and harmonic community for both traditional gamers and GameFi users for longevity and sustainability.

Socials

Website	https://krabots.io/
Telegram	https://t.me/Krabots_official
Twitter	https://twitter.com/Krabots
Medium	https://medium.com/@Krabots

Domain Info

Registrar Name	NameCheap, Inc.
Whois Server	whois.namecheap.com
Referral URL	https://www.namecheap.com/
Domain Expires On	2023-05-25
Domain Registered On	2022-05-25
Domain Updated On	2022-05-30
Servers Name	jean.ns.cloudflare.com 108.162.192.121 keenan.ns.cloudflare.com 172.64.35.11
Registrant Info	Redacted for privacy

Contract Details

Token Name	Krabots
Symbol	KRAC
Chain	BSC Mainnet
Contract Address	0xb91F0fdFfdDE4d6D53ac4066AcC32aA81fC6DE2C
Supply	100000000
Decimal	18
Creator Address	0x02c612a3556a372e84b16b57339c2a974bc5ca45
Owner Address	0x02c612a3556a372e84b16b57339c2a974bc5ca45
Buy tax	0%
Sell tax	0%

Security Analysis

Owner Can Set Fees	Security
Owner Can Mint Tokens	Security
Owner Can Burn Tokens	Security
Owner Can Blacklist	Security
Owner Can Whitelist	Security
Owner Can Set Transfers Cooldown	Security
Owner Can Pause Transfers	Security
Owner Can Take Back Ownership	Security
Proxy Contract	Security

Risk Levels

Critical	This level issue can lead to contract damage or functioning disruption. Immediate correction required.	**0**
High	This level issue can lead to smart contract manipulation. Fix required as soon as possible.	**0**
Medium	This level issue affects the required outcome of specific functions. The correction should be scheduled.	**0**
Low	This level issue does not affect the smart contract execution and can be ignored. No correction is required.	**1**

Contract Vulnerabilities (SWC-100 — SWC-117)

SWC-117	Signature Malleability	Passed
SWC-116	Block values as a proxy for time	Passed
SWC-115	Authorization through tx.origin	Passed
SWC-114	Transaction Order Dependence	Passed
SWC-113	DoS with Failed Call	Passed
SWC-112	Delegatecall to Untrusted Callee	Passed
SWC-111	Use of Deprecated Solidity Functions	Passed
SWC-110	Assert Violation	Passed
SWC-109	Uninitialized Storage Pointer	Passed
SWC-108	State Variable Default Visibility	Passed
SWC-107	Reentrancy	Passed
SWC-106	Unprotected SELFDESTRUCT Instruction	Passed
SWC-105	Unprotected Ether Withdrawal	Passed
SWC-104	Unchecked Call Return Value	Passed
SWC-103	Floating Pragma	Low
SWC-102	Outdated Compiler Version	Passed
SWC-101	Integer Overflow and Underflow	Passed
SWC-100	Function Default Visibility	Passed

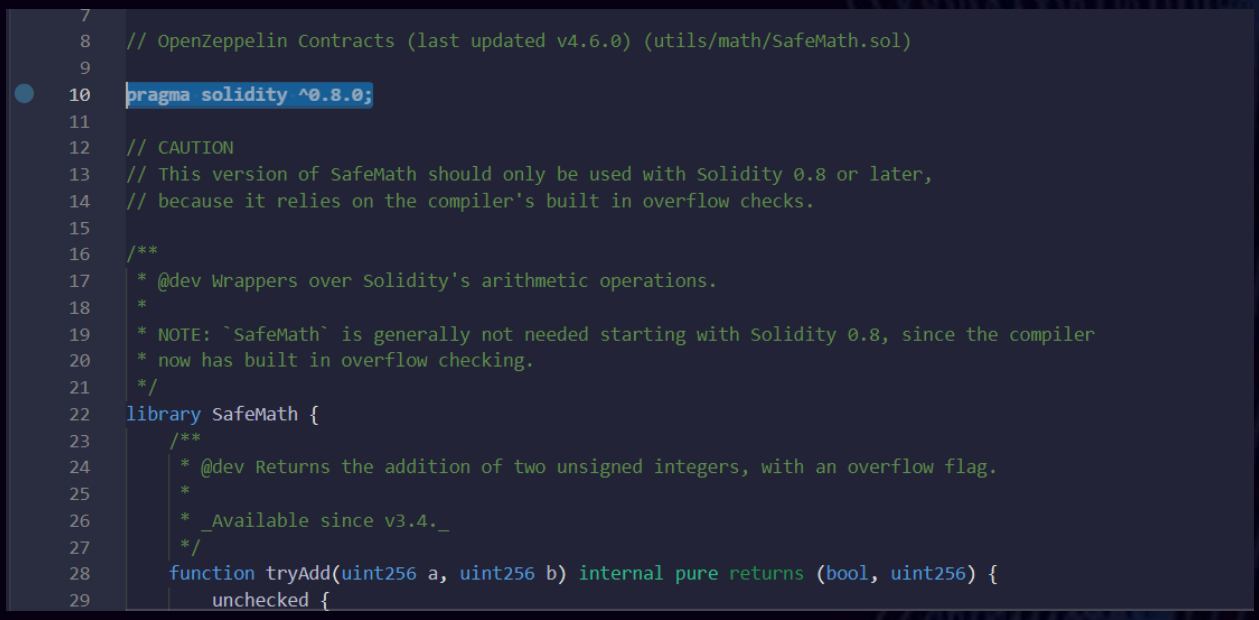
Contract Vulnerabilities (SWC-118 — SWC-136)

SWC-136	Unencrypted Private Data On-Chain	Passed
SWC-135	Code With No Effects	Passed
SWC-134	Message call with hardcoded gas amount	Passed
SWC-133	Hash Collisions With Multiple Variable Length Arguments	Passed
SWC-132	Unexpected Ether balance	Passed
SWC-131	Presence of unused variables	Passed
SWC-130	Right-To-Left-Override control character (U+202E)	Passed
SWC-129	Typographical Error	Passed
SWC-128	DoS With Block Gas Limit	Passed
SWC-127	Arbitrary Jump with Function Type Variable	Passed
SWC-126	Insufficient Gas Griefing	Passed
SWC-125	Incorrect Inheritance Order	Passed
SWC-124	Write to Arbitrary Storage Location	Passed
SWC-123	Requirement Violation	Passed
SWC-122	Lack of Proper Signature Verification	Passed
SWC-121	Missing Protection against Signature Replay Attacks	Passed
SWC-120	Weak Sources of Randomness from Chain Attributes	Passed
SWC-119	Shadowing State Variables	Passed
SWC-118	Incorrect Constructor Name	Passed

SWC-103

A Floating is Set

Low Security Issue –



```
// OpenZeppelin Contracts (last updated v4.6.0) (utils/math/SafeMath.sol)

pragma solidity ^0.8.0;

// CAUTION
// This version of SafeMath should only be used with Solidity 0.8 or later,
// because it relies on the compiler's built in overflow checks.

/**
 * @dev Wrappers over Solidity's arithmetic operations.
 *
 * NOTE: `SafeMath` is generally not needed starting with Solidity 0.8, since the compiler
 * now has built in overflow checking.
 */
library SafeMath {
    /**
     * @dev Returns the addition of two unsigned integers, with an overflow flag.
     *
     * _Available since v3.4._
     */
    function tryAdd(uint256 a, uint256 b) internal pure returns (bool, uint256) {
        unchecked {
```

The current pragma Solidity directive is "^0.8.0". It is recommended to specify a fixed compiler version to ensure that the bytecode produced does not vary between builds.

Conclusion

Contract Diagnostic

Low Severity issue: SWC-103.

This level issue does not affect the smart contract execution and can be ignored. No correction is required.

Contract Safety Analysis

Smart contract has an acceptable centralization risk.

Disclaimer

The goal of the current report is to make potential investors' research simpler. It should not be considered as a financial advice.

Chief Security Officer, Swiss Shield Labs
Bastien Moreau

Swiss Shield