SOLIDProof

*Bring trust into your projects*

**Blockchain Security | Smart Contract Audits | KYC Development | Marketing**

MADE IN GERMANY

# VEMP

# Audit

## Security Assessment

## 29. May, 2023

For

VEMP

# Disclaimer

SolidProof.io reports are not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. These reports are not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team. SolidProof.io do not cover testing or auditing the integration with external contract or services (such as Unicrypt, Uniswap, PancakeSwap etc’...)

**SolidProof.io Audits do not provide any warranty or guarantee regarding the absolute bug- free nature of the technology analyzed, nor do they provide any indication of the technology proprietors. SolidProof Audits should not be used in any way to make decisions around investment or involvement with any particular project. These reports in no way provide investment advice, nor should be leveraged as investment advice of any sort.**

SolidProof.io Reports represent an extensive auditing 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. SolidProof’s position is that each company and individual are responsible for their own due diligence and continuous security. SolidProof in no way claims any guarantee of security or functionality of the technology we agree to analyze.

| Version | Date | Description |
|---|---|---|
| 1.0 | 23. May 2022 | • Layout project<br>• Automated- /Manual-Security Testing<br>• Summary |
| 1.1 | 29. May 2023 | • Reaudit |

## Network
Ethereum (ERC20)

## Website
https://v-empire.io/

## Telegram
https://t.me/vempirediscussion

## Twitter
http://twitter.com/vempiredigital

## Medium
https://medium.com/@v-empire.digital

## Discord
https://discord.gg/Wk3aF3PNKM

## Youtube
https://youtube.com/c/vEmpireDDAO

## Description

VEMP Studios is the largest decentralized Metaverse investment organization. We are the world's first application that enables investors to earn interest on their Metaverse cryptocurrency holdings, paying yields in both VEMP and the original token staked. Alongside this, we're also the largest decentralized virtual real estate owner currently operating in the cryptocurrency industry. We also operate in the GameFi and NFT sectors and incubate new Metaverse, GameFi projects.

## Project Engagement

During the 18th of May 2022, **VEMP Team** engaged Solidproof.io to audit smart contracts that they created. The engagement was technical in nature and focused on identifying security flaws in the design and implementation of the contracts. They provided Solidproof.io with access to their code repository and whitepaper.

## Logo


## Contract Link

### v1.0

- https://goerli.etherscan.io/address/0x3297653ff5ad19b408bc18015e9ac179352a6dfe#code

### v1.1

https://github.com/v-Empire/vEmpire/blob/master/smart-contract/contractsV8/MasterChefLPPool.sol
Commit: 1faa5b2

# Vulnerability & Risk Level

Risk represents the probability that a certain source-threat will exploit vulnerability, and the impact of that event on the organization or system. Risk Level is computed based on CVSS version 3.0.

| Level | Value | Vulnerability | Risk (Required Action) |
|---|---|---|---|
| **Critical** | 9 - 10 | A vulnerability that can disrupt the contract functioning in a number of scenarios, or creates a risk that the contract may be broken. | Immediate action to reduce risk level. |
| **High** | 7 – 8.9 | A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way. | Implementation of corrective actions as soon aspossible. |
| **Medium** | 4 – 6.9 | A vulnerability that could affect the desired outcome of executing the contract in a specific scenario. | Implementation of corrective actions in a certain period. |
| **Low** | 2 – 3.9 | A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective. | Implementation of certain corrective actions or accepting the risk. |
| **Informational** | 0 – 1.9 | A vulnerability that have informational character but is not effecting any of the code. | An observation that does not determine a level of risk |

# Auditing Strategy and Techniques Applied

Throughout the review process, care was taken to evaluate the repository for security-related issues, code quality, and adherence to specification and best practices. To do so, reviewed line-by-line by our team of expert pentesters and smart contract developers, documenting any issues as there were discovered.

## Methodology

The auditing process follows a routine series of steps:

1. Code review that includes the following:
    i) Review of the specifications, sources, and instructions provided to SolidProof to make sure we understand the size, scope, and functionality of the smart contract.
    ii) Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
    iii) Comparison to specification, which is the process of checking whether the code does what the specifications, sources, and instructions provided to SolidProof describe.

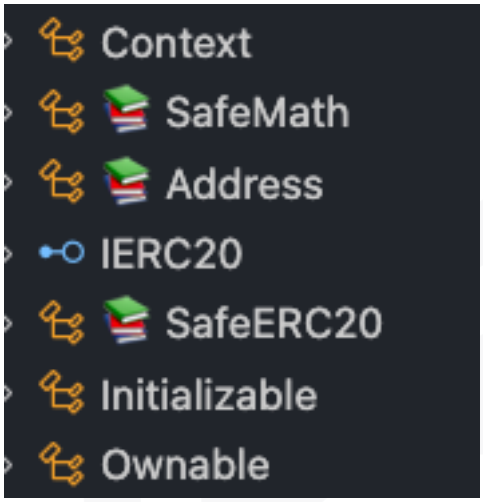
2. Testing and automated analysis that includes the following:
    i) Test coverage analysis, which is the process of determining whether the test cases are actually covering the code and how much code is exercised when we run those test cases.
    ii) Symbolic execution, which is analysing a program to determine what inputs causes each part of a program to execute.

3. Best practices review, which is a review of the smart contracts to improve efficiency, effectiveness, clarify, maintainability, security, and control based on the established industry and academic practices, recommendations, and research.

4. Specific, itemized, actionable recommendations to help you take steps to secure your smart contracts.

## Used Code from other Frameworks/Smart Contracts (direct imports)

Imported packages:



## Tested Contract Files

This audit covered the following files listed below with a SHA-1 Hash.

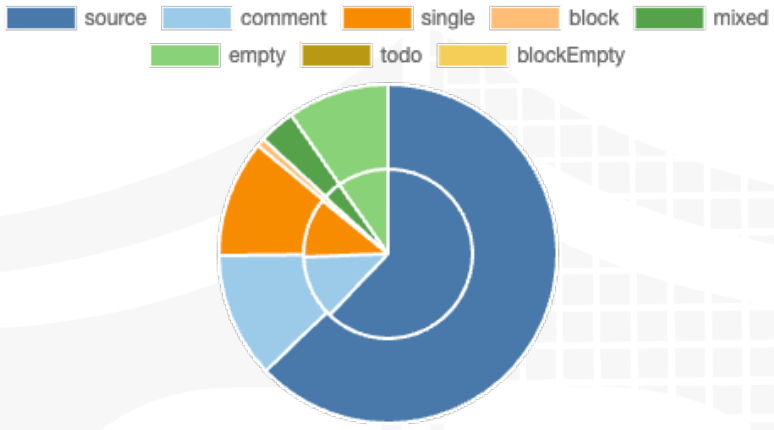
*A file with a different Hash has been modified, intentionally or otherwise, after the security review. A different Hash could be (but not necessarily) an indication of a changed condition or potential vulnerability that was not within the scope of this review.*

### v1.1

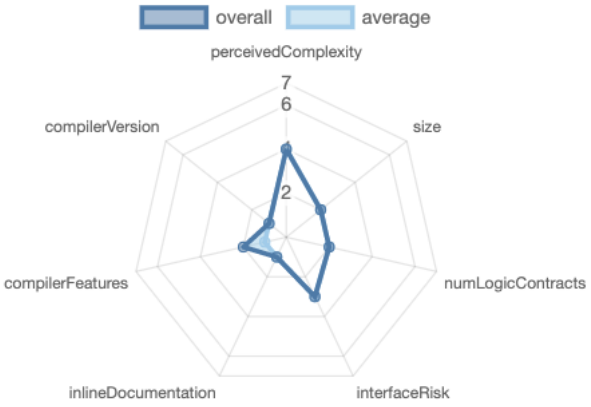
| File Name | SHA-1 Hash |
| --- | --- |
| contracts/ MasterChefLPPool.sol | b34ea6e8f50e3c7fa1c1de7f74111b52ebaa127d |

# Metrics

## Source Lines
### v1.0




## Risk Level
### v1.0



# Capabilities

## Components

| 📝Contracts | 📚Libraries | 🔍Interfaces | 💊Abstract |
|---|---|---|---|
| 2 | 3 | 1 | 2 |

### Exposed Functions

This section lists functions that are explicitly declared public or payable. Please note that getter methods for public stateVars are not included.

| 🌐Public | 💰Payable |
|---|---|
| 25 | 0 |

| External | Internal | Private | Pure | View |
|---|---|---|---|---|
| 8 | 65 | 3 | 15 | 12 |

### StateVariables

| Total | 🌐Public |
|---|---|
| 14 | 11 |

### Capabilities

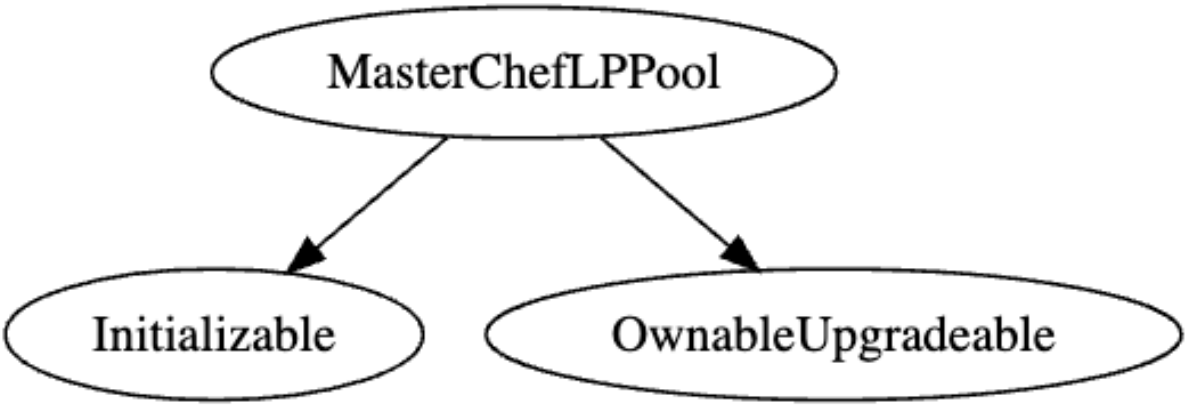
| Solidity Versions observed | 🧪 Experimental Features | 💰 Can Receive Funds | 🖥 Uses Assembly | 💣 Has Destroyable Contracts |
|---|---|---|---|---|
| `=0.6.12` | | | `yes` (2 asm blocks) | |

| 📩 Transfers ETH | ⚡ Low-Level Calls | 👥 DelegateCall | 🧮 Uses Hash Functions | 🦄 ECRecover | 🌀 New/Create/Create2 |
|---|---|---|---|---|---|
| `yes` | | `yes` | | | |

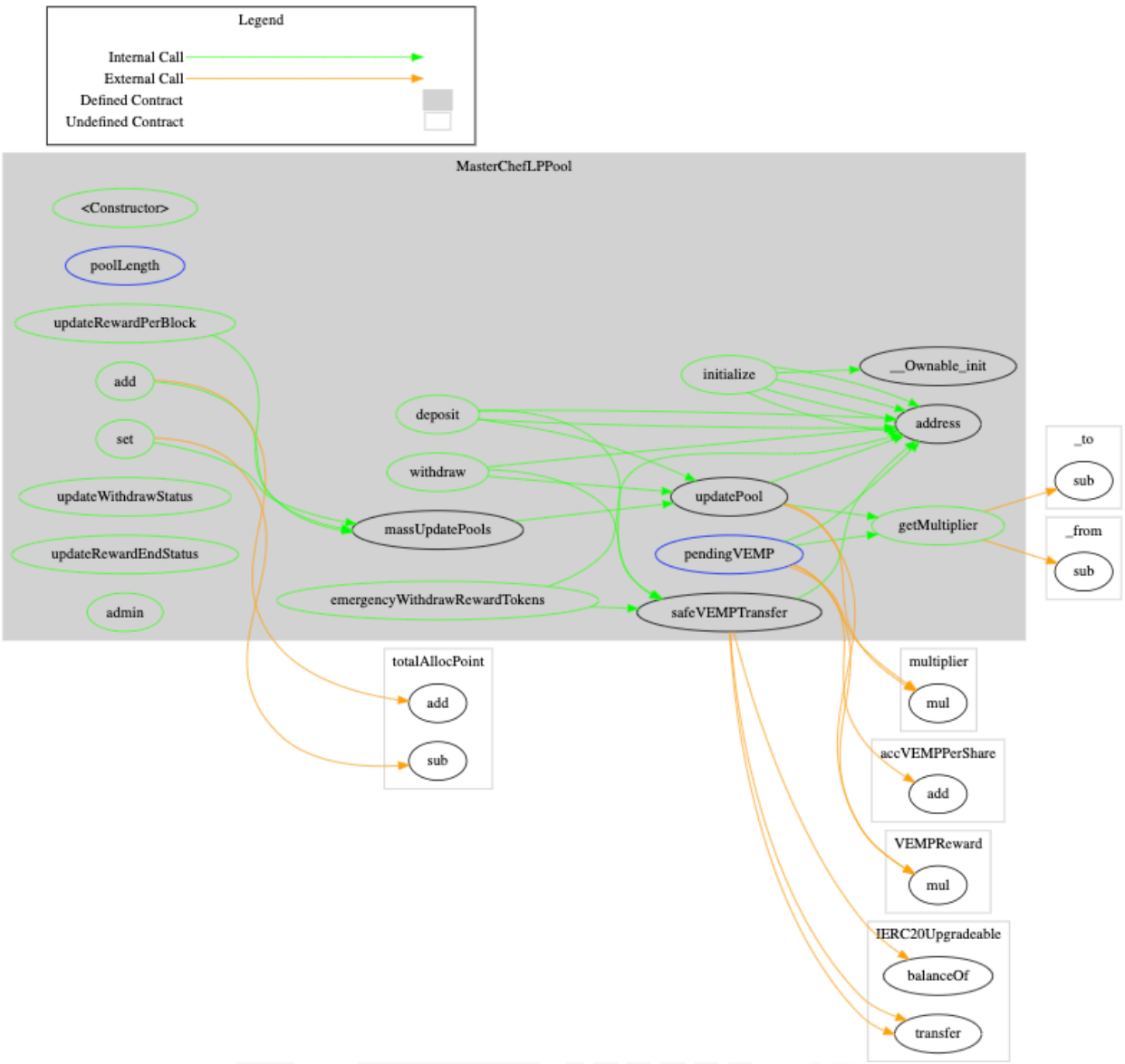
| ♻️ TryCatch | Σ Unchecked |
|---|---|
| | |

## Inheritance Graph

### v1.1



# CallGraph
## v1.1



## Scope of Work/Verify Claims

The above token Team provided us with the files that needs to be tested (Github, Bscscan, Etherscan, files, etc.). The scope of the audit is the main contract (usual the same name as team appended with .sol).

We will verify the following claims:

1. Is contract an upgradeable
2. Deployer cannot mint any new tokens
3. Deployer cannot burn or lock user funds
4. Deployer cannot pause the contract
5. Deployer cannot set fees
6. Deployer cannot blacklist/antisnipe addresses
7. Overall checkup (Smart Contract Security)

## Is contract an upgradeable

| Name | |
|---|---|
| Is contract an upgradeable? | Yes |

Comments:

**v1.1**

- Owner can deploy a new version of the contract which can change any limit and give owner new privileges
    - Be aware of this and do your own research for the contract which is the contract pointing to

## Write functions of contract v1.0

1. add (0x1eaaa045)
2. admin (0x63a846f8)
3. deposit (0xe2bbb158)
4. emergencyWithdrawRewardTokens (0xd0d6565d)
5. initialize (0xeb990c59)
6. massUpdatePools (0x630b5ba1)
7. renounceOwnership (0x715018a6)
8. set (0x64482f79)
9. transferOwnership (0xf2fde38b)
10. updatePool (0x51eb05a6)
11. updateRewardEndStatus (0xcc210cd3)
12. updateRewardPerBlock (0x01f8a976)
13. updateWithdrawStatus (0xbd674692)
14. withdraw (0x441a3e70)

## Deployer cannot mint any new tokens

| Name | Exist | Tested | Status |
|---|---|---|---|
| Deployer cannot mint | – | – | – |

## Deployer cannot burn or lock user funds

| Name | Exist | Tested | Status |
|---|---|---|---|
| Deployer cannot lock | ✓ | ✓ | ✓ |
| Deployer cannot burn | ✓ | ✓ | ✓ |

## Deployer cannot pause the contract

| Name | Exist | Tested | Status |
|---|---|---|---|
| Deployer cannot pause | – | – | – |

## Deployer cannot set fees

| Name | Exist | Tested | Status |
|---|---|---|---|
| Deployer cannot set fees over 25% | – | – | – |
| Deployer cannot set fees to nearly 100% or to 100% | – | – | – |

## Deployer can blacklist/antisnipe addresses

| Name | Exist | Tested | Status |
|---|---|---|---|
| Deployer cannot blacklist/antisnipe addresses | ✓ | ✓ | ✓ |

Comments:

**v1.0**

- Addresses cannot be blacklisted

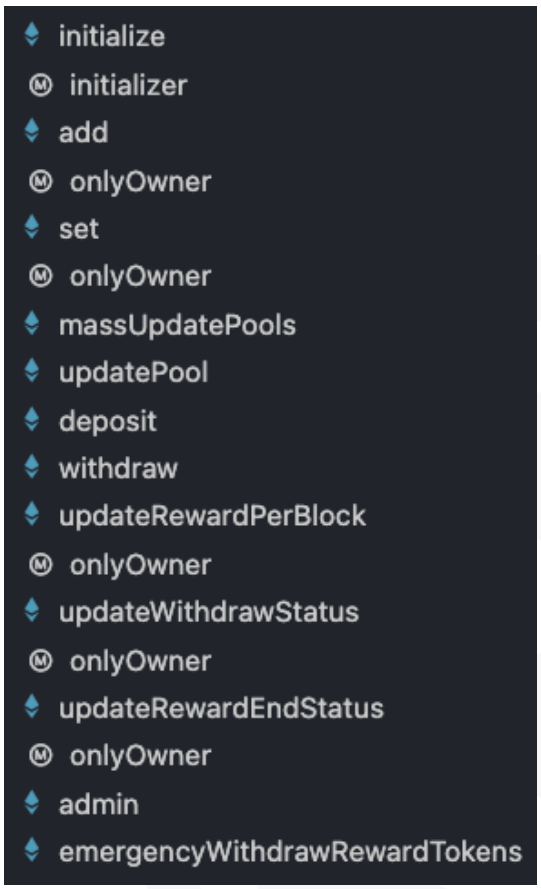
## Overall checkup (Smart Contract Security)

| Tested | Verified |
| --- | --- |
| ✓ | ✓ |

### Legend

| Attribute | Symbol |
| --- | --- |
| Verified / Checked | ✓ |
| Partly Verified | ⚑ |
| Unverified / Not checked | ✗ |
| Not available | - |

# Modifiers and public functions
## v1.0




## Ownership Privileges

- Add new LP to the pool
- Set a pool's allocation point
- Update reward per block to any arbitrary value including zero
- Update reward end status

**Please check if an OnlyOwner or similar restrictive modifier has been forgotten.**

# Source Units in Scope
## v1.0

| File | Logic Contracts | Interfaces | Lines | nLines | nSLOC | Comment Lines | Complex. Score |
|---|---|---|---|---|---|---|---|
| contracts/MasterChefLPPool.sol | 7 | 1 | 1114 | 924 | 468 | 468 | 281 |
| **Totals** | **7** | **1** | **1114** | **924** | **468** | **468** | **281** |

### Legend

| Attribute | Description |
|---|---|
| Lines | total lines of the source unit |
| nLines | normalised lines of the source unit (e.g. normalises functions spanning multiple lines) |
| nSLOC | normalised source lines of code (only source-code lines; no comments, no blank lines) |
| Comment Lines | lines containing single or block comments |
| Complexity Score | a custom complexity score derived from code statements that are known to introduce code complexity (branches, loops, calls, external interfaces, ...) |

# Audit Results

## Critical issues

**No critical issues**

## High issues

**No high issues**

## Medium issues

**Medium Issue Acknowledged**

| Issue | File | Type | Line | Description | Status |
|---|---|---|---|---|---|
| #1 | Main | Admin can withdraw staked tokens | 1109 | The admin address is able to withdraw staked tokens of the users which is not recommended. | Acknowledged |

## Low issues

| Issue | File | Type | Line | Description | Status |
|---|---|---|---|---|---|
| #1 | Main | Missing Events | 1089, 1103 | Emit Events for critical parameter changes. | Fixed |
| #2 | Main | Old Compiler Version | 7 | The contract uses a very old compiler version which is not recommended for deployment as it is susceptible to known vulnerabilities | Fixed |

## Informational issues

**No informational issues**

## Audit Comments

We recommend you use the special form of comments (NatSpec Format, Follow the link for more information https://docs.soliditylang.org/en/latest/natspec-format.html) for your contracts to provide rich documentation for

functions, return variables and more. This helps investors to make clear what that variable, functions etc. do.

## 29. May 2023:

- The owner can deploy a new version of the contract which can change any limit and give the owner new privileges
- Only the Owner can enable withdrawal in the contract.
- Read the whole report and modifiers section for more information

## SWC Attacks

| ID | Title | Relationships | Status |
|---|---|---|---|
| SWC-136 | Unencrypted Private Data On-Chain | CWE-767: Access to Critical Private Variable via Public Method | PASSED |
| SWC-135 | Code With No Effects | CWE-1164: Irrelevant Code | PASSED |
| SWC-134 | Message call with hardcoded gas amount | CWE-655: Improper Initialization | PASSED |
| SWC-133 | Hash Collisions With Multiple Variable Length Arguments | CWE-294: Authentication Bypass by Capture-replay | PASSED |
| SWC-132 | Unexpected Ether balance | CWE-667: Improper Locking | PASSED |
| SWC-131 | Presence of unused variables | CWE-1164: Irrelevant Code | PASSED |
| SWC-130 | Right-To-Left-Override control character (U+202E) | CWE-451: User Interface (UI) Misrepresentation of Critical Information | PASSED |
| SWC-129 | Typographical Error | CWE-480: Use of Incorrect Operator | PASSED |
| SWC-128 | DoS With Block Gas Limit | CWE-400: Uncontrolled Resource Consumption | PASSED |

| | | | |
|---|---|---|---|
| SWC-127 | Arbitrary Jump with Function Type Variable | CWE-695: Use of Low-Level Functionality | PASSED |
| SWC-125 | Incorrect Inheritance Order | CWE-696: Incorrect Behavior Order | PASSED |
| SWC-124 | Write to Arbitrary Storage Location | CWE-123: Write-what-where Condition | PASSED |
| SWC-123 | Requirement Violation | CWE-573: Improper Following of Specification by Caller | PASSED |
| SWC-122 | Lack of Proper Signature Verification | CWE-345: Insufficient Verification of Data Authenticity | PASSED |
| SWC-121 | Missing Protection against Signature Replay Attacks | CWE-347: Improper Verification of Cryptographic Signature | PASSED |
| SWC-120 | Weak Sources of Randomness from Chain Attributes | CWE-330: Use of Insufficiently Random Values | PASSED |
| SWC-119 | Shadowing State Variables | CWE-710: Improper Adherence to Coding Standards | PASSED |
| SWC-118 | Incorrect Constructor Name | CWE-665: Improper Initialization | PASSED |
| SWC-117 | Signature Malleability | CWE-347: Improper Verification of Cryptographic Signature | PASSED |

| | | | |
|---|---|---|---|
| SWC-116 | Timestamp Dependence | CWE-829: Inclusion of Functionality from Untrusted Control Sphere | PASSED |
| SWC-115 | Authorization through tx.origin | CWE-477: Use of Obsolete Function | PASSED |
| SWC-114 | Transaction Order Dependence | CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | PASSED |
| SWC-113 | DoS with Failed Call | CWE-703: Improper Check or Handling of Exceptional Conditions | PASSED |
| SWC-112 | Delegatecall to Untrusted Callee | CWE-829: Inclusion of Functionality from Untrusted Control Sphere | PASSED |
| SWC-111 | Use of Deprecated Solidity Functions | CWE-477: Use of Obsolete Function | PASSED |
| SWC-110 | Assert Violation | CWE-670: Always-Incorrect Control Flow Implementation | PASSED |
| SWC-109 | Uninitialized Storage Pointer | CWE-824: Access of Uninitialized Pointer | PASSED |
| SWC-108 | State Variable Default Visibility | CWE-710: Improper Adherence to Coding Standards | PASSED |
| SWC-107 | Reentrancy | CWE-841: Improper Enforcement of Behavioral Workflow | PASSED |
| SWC-106 | Unprotected SELFDESTRUCT Instruction | CWE-284: Improper Access Control | PASSED |

| | | | |
|---|---|---|---|
| SWC-105 | Unprotected Ether Withdrawal | CWE-284: Improper Access Control | PASSED |
| SWC-104 | Unchecked Call Return Value | CWE-252: Unchecked Return Value | PASSED |
| SWC-103 | Floating Pragma | CWE-664: Improper Control of a Resource Through its Lifetime | PASSED |
| SWC-102 | Outdated Compiler Version | CWE-937: Using Components with Known Vulnerabilities | PASSED |
| SWC-101 | Integer Overflow and Underflow | CWE-682: Incorrect Calculation | PASSED |
| SWC-100 | Function Default Visibility | CWE-710: Improper Adherence to Coding Standards | PASSED |