CERTIK

Security Assessment

The Fund

CertiK Assessed on Jul 17th, 2023

CertiK Assessed on Jul 17th, 2023

The Fund

The security assessment was prepared by CertiK, the leader in Web3.0 security.

Executive Summary

TYPES	ECOSYSTEM	METHODS
ERC-20	Ethereum (ETH)	Manual Review, Static Analysis

LANGUAGE	TIMELINE	KEY COMPONENTS
Solidity	Delivered on 07/17/2023	N/A

CODEBASE

https://github.com/dappd-net/the-fund/tree/fe43ddd552a4ed181e0349df8a8d1f524602af23

View All in Codebase Page

COMMITS

fe43ddd552a4ed181e0349df8a8d1f524602af23

b54584e881f713e645b48c680cb16e9ef33eceb4

3a6082d9d76d3ea239378cd8e4f662f5b4b8056e

View All in Codebase Page

Vulnerability Summary

3	2	0	0	1	0
Total Findings	Resolved	Mitigated	Partially Resolved	Acknowledged	Declined

0 Critical			Critical risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks.
1 Major	1 Acknowledged		Major risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project.
0 Medium			Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.
1 Minor	1 Resolved		Minor risks can be any of the above, but on a smaller scale. They generally do not compromise the overall integrity of the project, but they may be less efficient than other solutions.
1 Informational	1 Resolved		Informational errors are often recommendations to improve the style of the code or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

TABLE OF CONTENTS | THE FUND

Summary

Executive Summary

Vulnerability Summary

Codebase

Audit Scope

Approach & Methods

Third-Party Dependency

Description

Recommendations

Alleviation

Findings

FUN-04 : Centralization Risks in Fund.sol

FUN-01 : Unchecked ERC-20 `transfer()`/`transferFrom()` Call

FUN-03 : Potential Overflow

Optimizations

FUN-02 : User-Defined Getter

Appendix

Disclaimer

CODEBASE | THE FUND

Repository

https://github.com/dappd-net/the-fund/tree/fe43ddd552a4ed181e0349df8a8d1f524602af23

Commit

fe43ddd552a4ed181e0349df8a8d1f524602af23

b54584e881f713e645b48c680cb16e9ef33eceb4

3a6082d9d76d3ea239378cd8e4f662f5b4b8056e

AUDIT SCOPE | THE FUND

1 file audited ● 1 file with Acknowledged findings

ID	Repo	File	SHA256 Checksum
● FUN	dappd-net/the-fund	contracts/Fund.sol	586672816d055e3335e9b840244fae928441bf5a6d02e7ab5eee6a922a5fb7f0

APPROACH & METHODS | THE FUND

This report has been prepared for The Fund to discover issues and vulnerabilities in the source code of the The Fund project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Manual Review and Static Analysis 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.
- Thorough line-by-line manual review of the entire codebase by industry experts.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Testing the smart contracts against both common and uncommon attack vectors;
- Enhance general coding practices for better structures of source codes;
- Add enough unit tests to cover the possible use cases;
- Provide more comments per each function for readability, especially contracts that are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

THIRD-PARTY DEPENDENCY | THE FUND

Description

The contract is serving as the underlying entity to interact with one or more third party protocols. The scope of the audit treats third party entities as black boxes and assume their functional correctness. However, in the real world, third parties can be compromised and this may lead to lost or stolen assets. In addition, upgrades of third parties can possibly create severe impacts, such as increasing fees of third parties, migrating to new LP pools, etc.

```
238     IERC20 public immutable busd;
```

- The contract `Fund` interacts with third party contract with `IERC20` interface via `busd`.

```
446     function withdrawToken(address token) external onlyOwner {
```

- The function `Fund.withdrawToken` interacts with third party contract with `IERC20` interface via `token`.

Recommendations

We understand that the business logic requires interaction with the third parties. We encourage the team to constantly monitor the statuses of third parties to mitigate the side effects when unexpected activities are observed.

Alleviation

`[The Fund]`: This is a private contract where the funds are utilized for investing. Each member of The Fund is made aware of this fact with disclaimers on our page.

`[CertiK]`: In the latest commit of the codebase, `busd` has been switched to `USDC` with the ability to change the token in the future.

FINDINGS | THE FUND

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

This report has been prepared to discover issues and vulnerabilities for The Fund. Through this audit, we have uncovered 3 issues ranging from different severity levels. Utilizing the techniques of Manual Review & Static Analysis to complement rigorous manual code reviews, we discovered the following findings:

ID	Title	Category	Severity	Status
FUN-04	**Centralization Risks In Fund.Sol**	**Centralization**	**Major**	**Acknowledged**
FUN-01	Unchecked ERC-20 `transfer()` / `transferFrom()` Call	Volatile Code	Minor	Resolved
FUN-03	Potential Overflow	Incorrect Calculation	Informational	Resolved

FUN-04 | CENTRALIZATION RISKS IN FUND.SOL

Category	Severity	Location	Status
Centralization	**Major**	**contracts/Fund.sol: 59, 67, 435, 442, 446, 456, 467, 473, 481**	**Acknowledged**

Description

In the contract `Fund` the role `_owner` has authority over the functions shown below.

- `withdraw(uint256 amount)` : Withdraws specified amount of funds to team and dev wallets by `_owner` role
- `withdrawAll()` : Withdraws all funds to team and dev wallets by `_owner` role
- `withdrawToken(address token)` : Withdraws specified token balance to the owner by `_owner` role
- `setFundAddresses(address _fund, address _dev)` : Sets the fund and dev team wallet addresses by `_owner` role
- `setRoot(bytes32 _root)` : Sets the Merkle tree root for whitelisted users by `_owner` role
- `setDevFee(uint256 newFee)` : Sets the development fee by `_owner` role
- `setPackagePrice(uint newPrice)` : Sets the price per package by `_owner` role

In the contract `Ownable` the role `_owner` has authority over the functions shown below.

- `renounceOwnership()` : Allows the current owner to relinquish control of the contract by `_owner` role
- `transferOwnership(address newOwner)` : Transfers ownership of the contract to a new account by `_owner` role

Any compromise to the privileged account may allow the hacker to take advantage of this authority.

Recommendation

The risk describes the current project design and potentially makes iterations to improve in the security operation and level of decentralization, which in most cases cannot be resolved entirely at the present stage. We advise the client to carefully manage the privileged account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., multisignature wallets. Indicatively, here are some feasible suggestions that would also mitigate the potential risk at a different level in terms of short-term, long-term and permanent:

Short Term:

Timelock and Multi sign (⅔, ⅗) combination *mitigate* by delaying the sensitive operation and avoiding a single point of key management failure.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
  AND
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key compromised;
  AND
- A medium/blog link for sharing the timelock contract and multi-signers addresses information with the public audience.

Long Term:

Timelock and DAO, the combination, *mitigate* by applying decentralization and transparency.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
  AND
- Introduction of a DAO/governance/voting module to increase transparency and user involvement.
  AND
- A medium/blog link for sharing the timelock contract, multi-signers addresses, and DAO information with the public audience.

Permanent:

Renouncing the ownership or removing the function can be considered *fully resolved*.

- Renounce the ownership and never claim back the privileged roles.
  OR
- Remove the risky functionality.

FUN-01 | UNCHECKED ERC-20 `transfer()` / `transferFrom()` CALL

Category	Severity	Location	Status
Volatile Code	Minor	contracts/Fund.sol: 448, 491, 494	Resolved

Description

The return value of the transfer()/transferFrom() call is not checked.

```
448         IERC20(token).transfer(msg.sender, IERC20(token).balanceOf(address(this
)));
```

```
491             busd.transfer(fund, amountToFund);
```

```
494             busd.transfer(dev, amountToDev);
```

Recommendation

Since some ERC-20 tokens return no values and others return a `bool` value, they should be handled with care. We advise using the OpenZeppelin's `SafeERC20.sol` implementation to interact with the `transfer()` and `transferFrom()` functions of external ERC-20 tokens. The OpenZeppelin implementation checks for the existence of a return value and reverts if `false` is returned, making it compatible with all ERC-20 token implementations.

Alleviation

`[CertiK, 20230717]`: The team heeded the advice and resolved the finding in the commit 3a6082d9d76d3ea239378cd8e4f662f5b4b8056e

FUN-03 | POTENTIAL OVERFLOW

Category	Severity	Location	Status
Incorrect Calculation	Informational	contracts/Fund.sol: 320~329	Resolved

Description

In the function `deposit()`, the increment operation of `id`, `total` and `totalBUSD` are unchecked and therefore overflow of these values will not be protected. If any of these values increased to more than uint256.max, then overflow could happen.

Recommendation

We recommend the team check if the `id`, `total` and `totalBUSD` have any potential to be over than uint256.max. If yes, we recommend remove `unchecked` for `id`, `total` and `totalBUSD` variables in function `deposit()`

Alleviation

`[CertiK, 20230717]`: The team heeded the advice and resolved the finding in the commit 3a6082d9d76d3ea239378cd8e4f662f5b4b8056e

OPTIMIZATIONS | THE FUND

ID	Title	Category	Severity	Status
FUN-02	User-Defined Getter	Gas Optimization	Optimization	Resolved

FUN-02 | USER-DEFINED GETTER

Category	Severity	Location	Status
Gas Optimization	Optimization	contracts/Fund.sol: 404~406	Resolved

Description

```
 404  function getDepositIDs(address owner) external view returns (uint256[] memory)
{
 405      return userIDs[owner];
 406  }
```

The above function is equivalent to the compiler-generated getter function for the respective variable.

Recommendation

We advise that the linked variable is instead declared as `public` as compiler-generated getter function is less prone to error and much more maintainable than manually written one.

Alleviation

`[CertiK, 20230717]`: The team heeded the advice and resolved the finding in the commit 3a6082d9d76d3ea239378cd8e4f662f5b4b8056e

APPENDIX | THE FUND

Finding Categories

Categories	Description
Gas Optimization	Gas Optimization findings do not affect the functionality of the code but generate different, more optimal EVM opcodes resulting in a reduction on the total gas cost of a transaction.
Incorrect Calculation	Incorrect Calculation findings are about issues in numeric computation such as rounding errors, overflows, out-of-bounds and any computation that is not intended.
Volatile Code	Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases and may result in vulnerabilities.
Centralization	Centralization findings detail the design choices of designating privileged roles or other centralized controls over the code.

Checksum Calculation Method

The "Checksum" field in the "Audit Scope" section is calculated as the SHA-256 (Secure Hash Algorithm 2 with digest size of 256 bits) digest of the content of each file hosted in the listed source repository under the specified commit.

The result is hexadecimal encoded and is the same as the output of the Linux "sha256sum" command against the target file.

DISCLAIMER | CERTIK

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 CertiK'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 CertiK 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. CertiK's position is that each company and individual are responsible for their own due diligence and continuous security. CertiK'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 CertiK is 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, CERTIK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, CERTIK 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, CERTIK 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, CERTIK 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 CERTIK NOR ANY OF CERTIK'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. CERTIK 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 CERTIK'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 CERTIK WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF CERTIK 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 CERTIK 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.

CertiK | Securing the Web3 World

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we're able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.