Security Assessment

Universe Finance

Aug 14th, 2021

Table of Contents

Summary

This report has been prepared for Universe Finance to discover issues and vulnerabilities in the source code of the Universe Finance project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis and Manual Review 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:

- 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.

Overview

Project Summary

Project Name	Universe Finance
Description	Universe is a DeFi revenue product that focuses on Uniswap V3 liquidity management. It actively manages the liquidity of Uniswap V3 for you through smart strategies to safely and steadily increase liquidity mining revenue.
Platform	Ethereum
Language	Solidity
Codebase	https://github.com/UniverseFinance/UniverseFinanceProtocol https://etherscan.io/address/0x5c0E6Eefa871aD08BFfd1F1CdDE7B808103a38ba https://etherscan.io/address/0x39A88389Ae0A307b9E4041d8778c8bf1ebCd54D6
Commit	579bf020a042863641ec30aaceb65a047c04777f

Audit Summary

Delivery Date	Aug 14, 2021
Audit Methodology	Static Analysis, Manual Review
Key Components	

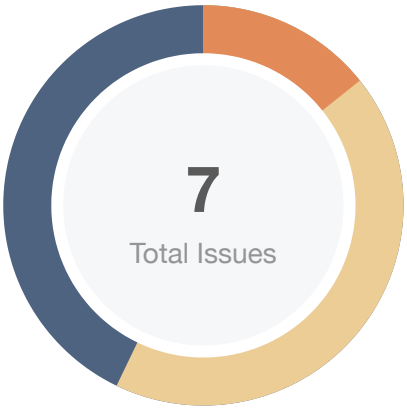
Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Partially Resolved	Resolved
Critical	0	0	0	0	0	0
Major	1	0	0	0	0	1
Medium	0	0	0	0	0	0
Minor	3	0	0	1	0	2
Informational	3	0	0	0	0	3
Discussion	0	0	0	0	0	0

Audit Scope

ID	File	SHA256 Checksum
GVU	GeneralVault.sol	e95fca906e1514a9a5559ea8ca7f6a68dacab688c4a8b523c5f4ce6ce7a89686
SIS	SingleIntervalStrategy.sol	bd6f64687fd90daf874dea32ecbdcde11477e6b8f30586001dcc076b3c31fd9b

Findings



Critical	**0** (0.00%)
Major	**1** (14.29%)
Medium	**0** (0.00%)
Minor	**3** (42.86%)
Informational	**3** (42.86%)
Discussion	**0** (0.00%)

ID	Title	Category	Severity	Status
GVU-01	Function Optimization	Control Flow	Informational	Resolved
GVU-02	Privileged ownership	**Centralization / Privilege**	**Major**	Resolved
GVU-03	Missing Emit Events	Coding Style	Informational	Resolved
SIS-01	External dependency	Logical Issue	Minor	Acknowledged
SIS-02	Logic Issue	Logical Issue	Minor	Resolved
SIS-03	Comparison with boolean	Logical Issue	Informational	Resolved
UFE-01	Financial Models	Logical Issue	Minor	Resolved

GVU-01 | Function Optimization

Category	Severity	Location	Status
Control Flow	Informational	GeneralVault.sol: 162~184	Resolved

Description

The function `combineAmount()` is only called in the function `_calcShare()`, the input parameters `total0` and `total1` have been restricted to not equal to 0, so the following judgment statement is redundant.

```
171     if (total0 == 0) {
172         amount0Desired = amount0Desired.mul(997).div(1000);
173       } else if (total1 == 0) {
174         amount1Desired = amount1Desired.mul(997).div(1000);
175       }
```

Recommendation

We recommend optimizing this function for the actual situation to enhance readability.

Alleviation

The team heeded the advice and resolved this issue in commit `3f1e8eb1cf56fb57d07a93e6d0ef45b9827ddbc8`.

GVU-02 | Privileged ownership

Category	Severity	Location	Status
Centralization / Privilege	**Major**	GeneralVault.sol	Resolved

Description

The owner of contract `GeneralVault` has the permission to:

1. `changeStrategy` - change the address of strategy contract

without obtaining the consensus of the community.

Recommendation

We advise the client to carefully manage the `governance/guardian` account's private key to avoid any potential risks of being hacked.

In general, we strongly recommend centralized privileges or roles in the protocol to be improved via a decentralized mechanism or via smart-contract-based accounts with enhanced security practices, e.g. Multisignature wallets.

Here are some feasible solutions that would also mitigate the potential risk:

- Time-lock with reasonable latency, i.e. 48 hours, for awareness on privileged operations;
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key;
- Introduction of a DAO/governance/voting module to increase transparency and user involvement.

Alleviation

The team removed the function in commit `4977996af58fe8656023ebf805f8f82010840635`.

GVU-03 | Missing Emit Events

Category	Severity	Location	Status
Coding Style	Informational	GeneralVault.sol: 61	Resolved

Description

Functions that affect the status of sensitive variables should be able to emit events as notifications to customers:

- `changeDev()`
- `changeOperator()`

Recommendation

We advise the client to consider adding events for sensitive actions, and emit them.

Alleviation

The team heeded the advice and resolved this issue in commit `246a1ce23e6bb8b18ef3d662912553b4bb879a2d`.

SIS-01 | External dependency

Category	Severity	Location	Status
Logical Issue	Minor	SingleIntervalStrategy.sol: 83	Acknowledged

Description

The contract is serving as the underlying entity to interact with external dependencies `IUniswapV3Pool` and `ISwapRouter` protocols. The scope of the audit would treat those external dependencies entities as black boxes and assume the functional correctness. In fact, any external dependencies might be compromised that led to assets lost or stolen.

Recommendation

We encourage the team to constantly monitor the statuses of those external dependencies to mitigate the side effects when unexpected activities are observed.

Alleviation

[UniverseFinance]: Our project relies on `UniswapV3Pool` and `SwapRouter`, and we've already browsed their code.

SIS-02 | Logic Issue

Category	Severity	Location	Status
Logical Issue	Minor	SingleIntervalStrategy.sol: 428~429	Resolved

Description

Function `mining()` is an external function that anyone can call, and you should add code to verify that the `sender` in the `whiteList` and that its corresponding `config` is valid.

If the `config` is invalid, the following code is still executing, and there seems to be no code to throw an exception warning about it.

There is also described in the code comment: `check config`.

Recommendation

We recommend adding verification to verify that the caller is in the `whiteList`.

Alleviation

The team heeded the advice and resolved this issue in commit `316d057933d5e7fbfa1f888572ad8e8abf55b683`.

SIS-03 | Comparison with boolean

Category	Severity	Location	Status
Logical Issue	Informational	SingleIntervalStrategy.sol: 57	Resolved

Description

Performs comparison with a boolean literal `true` which can be replaced with affirmative of the expression to increase the legibility of the codebase.

Recommendation

Consider modifying like below:

```
1  require(whiteLists[msg.sender], "onlyWhiteList Vault");
```

Alleviation

The team heeded the advice and resolved this issue in commit `54ad97c09b76bf4c688935e27d22eaa762ab3b98`.

UFE-01 | Financial Models

Category	Severity	Location	Status
Logical Issue	Minor	../.. (undefined)	Resolved

Description

There are three aspects of the financial model that need to be discussed:

- The user deposits a certain amount of token0 and token1 into the strategy contract and earns income by providing liquidity in the uniswapV3 pool. In addition to this part, what kind of income does the user have?
- In the mining method of the strategy contract, after providing liquidity, the excess token0 and token1 will be transferred back to the vault contract. This part of the tokens can either be distributed proportionally when the user withdraws or can be revested into the strategy, how do these two methods achieve a balance?
- The introduction document of the project mentioned that Universe can automatically `reBalance` and automatically `reInvest`, but in the vault contract, these two methods are both manually invoked.

Recommendation

Financial models of blockchain protocols need to be resilient to attacks. It needs to pass simulations and verifications to guarantee the security of the overall protocol.

Alleviation

[Universe Finance Team]:

- The income of the user is the fee obtained by univ3 pledging liquidity, the fee includes two types of tokens. The distribution is conducted exactly according to the share of ULP held by the user.
- There are fractions that cannot be avoided when pledging, so we can only deposit these fractions in the vault contract, and these fractions will be returned to the user when he withdraws them. Our initial intention is to put the money into mining as much as possible, but fractions are unavoidable, as long as the attribution of the money is clearly calculated.
- We will modify the introduction document to make the description more accurate.

Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on how block.timestamp works.

Control Flow

Control Flow findings concern the access control imposed on functions, such as owner-only functions being invoke-able by anyone under certain circumstances.

Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to make the codebase more legible and, as a result, easily maintainable.

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

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.

About

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.