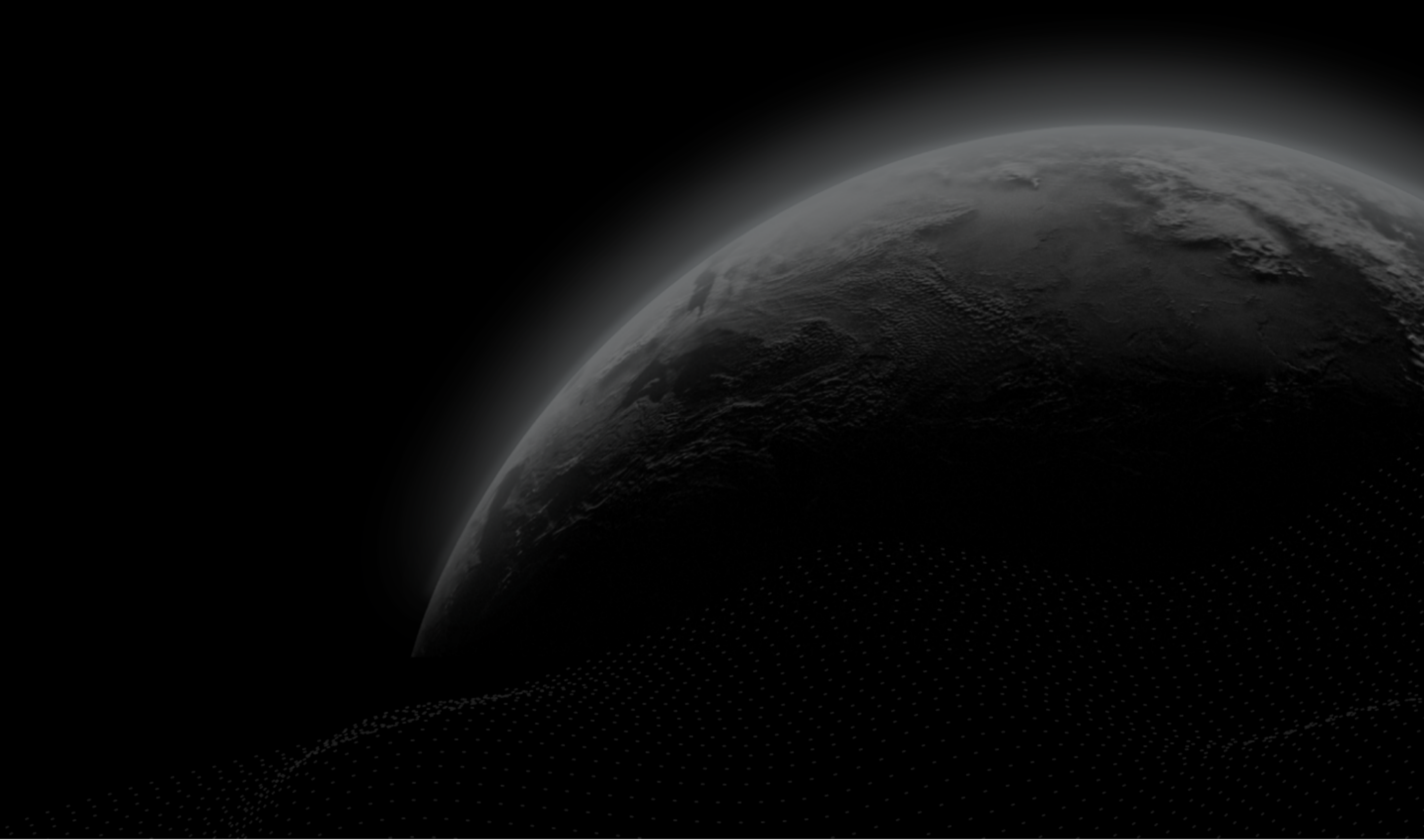
CERTIK

Security Assessment

Venus - Isolated Pools Allow Multiple Rewards Distributors

CertiK Assessed on Aug 24th, 2023



CertiK Assessed on Aug 24th, 2023

Venus - Isolated Pools Allow Multiple Rewards Distributors

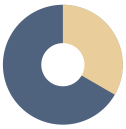
The security assessment was prepared by CertiK, the leader in Web3.0 security.

Executive Summary

TYPES	ECOSYSTEM	METHODS
DeFi	Binance Smart Chain (BSC)	Manual Review, Static Analysis
LANGUAGE	**TIMELINE**	**KEY COMPONENTS**
Solidity	Delivered on 08/24/2023	N/A

CODEBASE	COMMITS
https://github.com/VenusProtocol/isolated-pools/	7603b4ed84040dd883aa3a8f411dd2d2d1fb4956
View All in Codebase Page	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.
🟧	0	Major		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 Acknowledged	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.
🟦	2	Informational	2 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

VENUS - ISOLATED POOLS ALLOW MULTIPLE REWARDS DISTRIBUTORS

CODEBASE | VENUS - ISOLATED POOLS ALLOW MULTIPLE REWARDS DISTRIBUTORS

Repository

https://github.com/VenusProtocol/isolated-pools/

Commit

7603b4ed84040dd883aa3a8f411dd2d2d1fb4956

AUDIT SCOPE | VENUS - ISOLATED POOLS ALLOW MULTIPLE REWARDS DISTRIBUTORS

1 file audited ● 1 file with Acknowledged findings

ID	Repo	File	SHA256 Checksum
● CVP	VenusProtocol/isolated-pools	contracts/Comptroller.sol	700f492c0937a0ff249e683649bccd14aab9ec78b636d24919baef5f2bc9ae8d

APPROACH & METHODS | VENUS - ISOLATED POOLS ALLOW MULTIPLE REWARDS DISTRIBUTORS

This report has been prepared for Venus to discover issues and vulnerabilities in the source code of the Venus - Isolated Pools Allow Multiple Rewards Distributors 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.

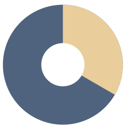
SUMMARY | VENUS - ISOLATED POOLS ALLOW MULTIPLE REWARDS DISTRIBUTORS

This audit concerns the changes made in files outlined in this PR: https://github.com/VenusProtocol/isolated-pools/pull/290.

The change made in this PR was to allow multiple rewards distributors to have the same reward token. This was done by removing the check that a new rewards distributor's reward token was not the reward token of a rewards distributor that have previously been added.

As the audit report was concerned only with changes introduced in this PR, it did not take any centralization risk or other dependencies into consideration. We recommend users review all previous audits here: https://skynet.certik.com/projects/venus.

FINDINGS | VENUS - ISOLATED POOLS ALLOW MULTIPLE REWARDS DISTRIBUTORS



3	0	0	0	1	2
Total Findings	Critical	Major	Medium	Minor	Informational

This report has been prepared to discover issues and vulnerabilities for Venus - Isolated Pools Allow Multiple Rewards Distributors. 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
CVP-01	`rewardsDistributors` Array May Contain Inactive Distributors	Logical Issue	Minor	● Acknowledged
CVP-02	Other Protocols May Assume There Is A Single `RewardsDistributor` Per Reward Token	Logical Issue	Informational	● Resolved
CVP-03	Possible To Have Multiple Rewards Distributors Issuing Same Reward Token At Same Time	Logical Issue	Informational	● Resolved

CVP-01 | `rewardsDistributors` ARRAY MAY CONTAIN INACTIVE DISTRIBUTORS

Category	Severity	Location	Status
Logical Issue	● Minor	contracts/Comptroller.sol: 968~969	● Acknowledged

Description

If multiple rewards distributors are allowed for the same token, this may cause the `rewardsDistributors` array to grow excessively large. As the hooks iterate through the entire `rewardsDistributors` array, this may cost a significant amount of gas to be used unnecessarily. In addition, if enough `rewardsDistributors` are added, then this will cause the max loops to need to be adjusted, which may cause issues with other loops that are not dependent on the size of the `rewardsDistributors` array.

Recommendation

Note that this is only an issue when the amount of `rewardsDistributors` significantly exceeds the amount of markets or there is a significant amount of inactive `rewardsDistributors`.

We recommend adding a method to track the active distributors, that is, those distributors who should still be called by the comptroller's hooks. Then the comptroller hooks can iterate only through the active distributors, while the `rewardsDistributors` array can still keep a record of all rewards distributors.

Alleviation

`[Venus, 08/24/2023]`: Issue acknowledged. I won't make any changes for the current version.

We prefer to keep it as it is now and we'll consider a change if the number of RewardsDistributor grows too much in the future.

CVP-02 | OTHER PROTOCOLS MAY ASSUME THERE IS A SINGLE `RewardsDistributor` PER REWARD TOKEN

Category	Severity	Location	Status
Logical Issue	● Informational	contracts/Comptroller.sol: 966	● Resolved

Description

There may be protocols that interact with Venus Isolated-Pools that based their design on the assumption that there is a single `RewardsDistributor` per reward token. For example, they may use a mapping from the reward token to the `RewardsDistributor`, which will not allow them to handle scenarios where there are multiple rewards distributors.

Recommendation

We recommend making a public announcement about this change and how it may cause compatibility issues with any protocol that based their design on this assumption. In addition, we recommend reaching out to any partners to ensure that they did not make design choices based on this assumption and that this change will not significantly affect the functionality of their protocol.

Alleviation

`[CertiK, 08/24/2023]` : The client added comments to the function explaining the new functionality in commit: 3bd2009ddd8577b015263bf082685fa6be113e43 and stated the following regarding informing the public:

`[Venus, 08/24/2023]` : We'll also update the public documentation site (http://docs-v4.venus.io) with this content.

See the commit here: 3576ad14095350f872e414d60313de42371cab9f.

CVP-03 | POSSIBLE TO HAVE MULTIPLE REWARDS DISTRIBUTORS ISSUING SAME REWARD TOKEN AT SAME TIME

Category	Severity	Location	Status
Logical Issue	● Informational	contracts/Comptroller.sol: 966	● Resolved

Description

Currently it is possible to add two distinct rewards distributors that will have the same reward token and have an overlap in the blocks in which the rewards will be distributed. As the reward token speeds and last reward block can be adjusted, a single rewards distributor can be used in the case that there is an overlap in rewards.

Recommendation

We recommend disallowing overlapping rewards for the same token over reward distributors. If the other solutions provided in the other findings present within the report are adopted, then this can be done by ensuring there is at most one active rewards distributor for a given reward token at a time. Alternatively, we recommend only creating multiple reward distributors when necessary to minimize the total amount of rewards distributors.

Alleviation

`[Venus, 08/24/2023]` : This is the expected behaviour. If there is an overlap and we can reuse the same RewardsDistributor contract, we'll do it, extending the last reward block, for example.

But sometimes it's not easy to use only one RewardsDistributor contract. For example, if the distribution speeds are different in RewardsDistributor contract 1 and contract 2, taking into account the changes in the contracts are done with VIP's (it means, without precision on the specific blocks when the changes are done), we won't be able to configure the different speeds correctly. In that case, it would be better to use two different RewardsDistributor contracts.

`[CertiK, 08/24/2023]` : Considering these cases, we agree that there are valid use cases for allowing multiple active `RewardsDistributor` contracts for the same reward token and mark this finding as *resolved*. However, we recommend keeping a single active `RewardsDistributor` per reward token whenever possible.

APPENDIX | VENUS - ISOLATED POOLS ALLOW MULTIPLE REWARDS DISTRIBUTORS

Finding Categories

Categories	Description
Logical Issue	Logical Issue findings indicate general implementation issues related to the program logic.

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.