Venus - ERC4626Oracle

Security Assessment

CertiK Assessed on Feb 6th, 2025

CertiK Assessed on Feb 6th, 2025

Venus - ERC4626Oracle

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 02/06/2025	N/A

CODEBASE
https://github.com/VenusProtocol/oracle
View All in Codebase Page

COMMITS
Base: 26ce2b4ad4867230cb667b4bda9d864e5164a6d5
View All in Codebase Page

Vulnerability Summary

3	0	0	0	3	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 Acknowledged	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 - ERC4626ORACLE

CODEBASE | VENUS - ERC4626ORACLE

Repository

https://github.com/VenusProtocol/oracle

Commit

Base: 26ce2b4ad4867230cb667b4bda9d864e5164a6d5

AUDIT SCOPE | VENUS - ERC4626ORACLE

1 file audited • 1 file without findings

ID	Repo	File	SHA256 Checksum
ERC	VenusProtocol/oracle	ERC4626Oracle.sol	418e36130c12ffcd433e22a1926d2ae23b6edbd89da3728c15a0213e0a91047a

APPROACH & METHODS | VENUS - ERC4626ORACLE

This report has been prepared for Venus to discover issues and vulnerabilities in the source code of the Venus - ERC4626Oracle 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 - ERC4626ORACLE

This audit concerns the changes made in files outlined in:

- PR-253

Note that any centralization risks present in the existing codebase before these PRs were not considered in this audit and only those added in these PRs are addressed in the audit. We recommend all users carefully review the centralization risks, much of which can be found in our previous audits, which can be found here: https://skynet.certik.com/projects/venus.

The `ERC4626Oracle` is designed to return the price of ERC-4626 tokens. This contract utilizes the `convertToAssets()` function of the ERC-4626 vault to convert 1 share to the corresponding amount of underlying assets. This converted value is then multiplied by the price of the underlying asset obtained via the resilient oracle.

It is important to note that not all ERC4626 tokens are compatible and that supported tokens should be thoroughly vetted. See the finding **Supported ERC-4626 Tokens Must Be Compatible With The Oracle** for more details.

DEPENDENCIES | VENUS - ERC4626ORACLE

Third Party Dependencies

The protocol is serving as the underlying entity to interact with third party protocols. The third parties that the contracts interact with are:

- Third Party ERC20 Contracts
- Third Party ERC4626 Contracts
- Third Party Oracles

The scope of the audit treats third party entities as black boxes and assumes their functional correctness. However, in the real world, third parties can be compromised and this may lead to lost or stolen assets. Moreover, updates to the state of a project contract that are dependent on the read of the state of external third party contracts may make the project vulnerable to read-only reentrancy. In addition, upgrades of third parties can possibly create severe impacts, such as returning invalid prices, returning invalid exchange rates, etc.

Out Of Scope Dependencies

The protocol is serving as the underlying entity to interact with out-of-scope dependencies. The out-of-scope dependencies that the contracts interact with are:

- Resilient Oracle

The scope of the audit treats out-of-scope dependencies as black boxes and assumes their functional correctness.

Recommendations

We recommend constantly monitoring the third parties involved to mitigate any side effects that may occur when unexpected changes are introduced, as well as vetting any third party contracts used to ensure no external calls can be made before updates to its state. Additionally, we recommend all out-of-scope dependencies are carefully vetted to ensure they function as intended.

FINDINGS | VENUS - ERC4626ORACLE

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 - ERC4626Oracle. 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
ERC-01	Missing Input Validation	Logical Issue	Minor	Acknowledged
ERC-02	Supported ERC-4626 Tokens Must Be Compatible With The Oracle	Logical Issue	Informational	Acknowledged
ERC-03	ERC4626 Vaults May Have Decimals Greater Than 18	Logical Issue	Informational	Acknowledged

ERC-01 | MISSING INPUT VALIDATION

Category	Severity	Location	Status
Logical Issue	Minor	ERC4626Oracle.sol: 21	Acknowledged

Description

The `correlatedToken` is assumed to be an ERC4626 vault, and the input `underlyingToken` must be the asset of the vault. However, it is not checked that the asset of the vault is the input `underlyingToken`. If the incorrect `underlyingToken` is chosen, it will result in an incorrect underlying amount returned and thus will result in inaccurate pricing.

Recommendation

We recommend adding the input validations above to prevent unexpected errors. In addition, we recommend adding comments that the input `correlatedToken` must be an `ERC4626` vault.

Alleviation

`[Venus, 02/06/2025]`: "The current code allows us to assume some token equivalences, and reuse some prices. For example, if the underlying token of the ERC4626 token would be stETH, we would like to assume stETH 1:1 ETH, and configure WETH as the underlying asset of our ERC4626 oracle.

There are several layers of review (Risk managers, Venus labs team, Community) before these oracles are enabled on mainnet. We prefer to delegate the assessment of the configuration to that review process, instead of forcing it on the code."

ERC-02 | SUPPORTED ERC-4626 TOKENS MUST BE COMPATIBLE WITH THE ORACLE

Category	Severity	Location	Status
Logical Issue	Informational	ERC4626Oracle.sol: 21	Acknowledged

Description

The `ERC4626Oracle` contract relies on the security of the underlying ERC-4626 implementation and the behavior of the `convertToAssets()` function. The following specifications should be ensured for every ERC4626 token that is to be supported with this oracle.

- It **must** comply with the ERC-4626 specification.
- It **should** have been audited and is free from share manipulation vulnerabilities. In particular direct or stealth donation attack vectors should be properly mitigated.
- It **should** be non-upgradeable or if it is upgradeable the upgrade authority should be well trusted and carefully monitored.
- It **should not** incorporate fees, otherwise, `convertToAssets()` may return an inflated share price as it does not account for the fees charged.
- It **should not** incorporate custom logic, such as delayed withdrawals or other constraints that can affect share value. Such mechanisms result in the share value being less than the amount of assets they can be redeemed for due to the delay and available liquidity. Vaults using other custom logic should be considered on a case by case basis to ensure proper integration.
- It **should not** include flash loan functionality. If the vault allows flash loans, then during the flash loan the vaults balance will decrease and may manipulate the return value of `convertToAssets()`.
- It **should be** highly liquid to ensure negligible slippage when converting shares to assets and vice versa. Otherwise, `convertToAssets()` may be inflated.

Recommendation

We recommend ensuring that all ERC4626 tokens that will be supported follow the specifications above.

Alleviation

`[Venus, 02/06/2025]`: "We'll incorporate the suggested checks to the list of pre-checks already performed when a new market is evaluated."

ERC-03 | ERC4626 VAULTS MAY HAVE DECIMALS GREATER THAN 18

Category	Severity	Location	Status
Logical Issue	Informational	ERC4626Oracle.sol: 22	Acknowledged

Description

Some ERC4626 implementations, such as OpenZeppelin's, may have more than 18 decimals. For example, if the OZ implementation is used on an asset that has 18 decimals and the decimal offset is chosen to be 1, then the ERC4626 token will have 19 decimals. (See here).

There are assumptions made throughout the codebase that the decimals of tokens are less than or equal to 18. If such an ERC4626 token is to be supported, we recommend carefully reviewing to ensure that it does not cause any potential issues within the protocol.

Recommendation

We recommend carefully reviewing each ERC4626 token to be supported and if the decimals are greater than 18, ensuring it properly integrates within the entire protocol.

Alleviation

`[Venus, 02/06/2025]`: "Venus doesn't support underlying tokens with more than 18 decimals. We (Community, Venus Labs, Risk managers) review it before adding new markets."

APPENDIX | VENUS - ERC4626ORACLE

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.

Elevating Your Entire Web3 Journey

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.