



Venus WstETHOracleV2 Upgrade

Security Assessment

CertiK Assessed on Jun 23rd, 2025





Certik Assessed on Jun 23rd, 2025

Venus WstETHOracleV2 Upgrade

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

Executive Summary

TYPES

Lending

ECOSYSTEM

Binance Smart Chain
(BSC)

METHODS

Manual Review, Static Analysis

LANGUAGE

Solidity

TIMELINE

Delivered on 06/23/2025

KEY COMPONENTS

N/A

CODEBASE

<https://github.com/VenusProtocol/oracle>

View All in Codebase Page

COMMITTS

Base: [43179a0ddaaacb52ca3130efcb9cd36246bb45](#)Update1: [dbf8fc5854632b08e187cf76af876926eb20541f](#)

View All in Codebase Page

Vulnerability Summary



3

Total Findings

2

Resolved

0

Partially Resolved

1

Acknowledged

0

Declined

0 Centralization

Centralization findings highlight privileged roles & functions and their capabilities, or instances where the project takes custody of users' assets.

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 may include logical errors that, under specific circumstances, could result in fund losses or loss of project control.

0 Medium

Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.

0 Minor

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.

3 Informational

2 Resolved, 1 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 WSTETHORACLEV2 UPGRADE

I Summary

[Executive Summary](#)

[Vulnerability Summary](#)

[Codebase](#)

[Audit Scope](#)

[Approach & Methods](#)

I Overview

I Dependencies

[Third Party Dependencies](#)

[Recommendations](#)

I Findings

[VWU-01 : `underlyingToken` Should Be Carefully Configured](#)

[VWU-02 : Typos And Inconsistencies](#)

[VWU-03 : Risks If `stETH` Market Price Declines Significantly](#)

I Appendix

I Disclaimer

CODEBASE | VENUS WSTETHORACLEV2 UPGRADE

Repository

<https://github.com/VenusProtocol/oracle>


Commit

Base: [43179a0ddaaacb52ca3130efcb9cd36246bb45](#)

Update1: [dbf8fc5854632b08e187cf76af876926eb20541f](#)

AUDIT SCOPE | VENUS WSTETHORACLEV2 UPGRADE

1 file audited ● 1 file without findings

ID	Repo	File	SHA256 Checksum
● WET	VenusProtocol/oracle	 WstETHOracleV2.sol	9b596ae9bad811283d5b4159a847dad3c4 f861cdfde9e308e1a0ea7c741e4e26

APPROACH & METHODS | VENUS WSTETHORACLEV2 UPGRADE

This report has been prepared for Venus to discover issues and vulnerabilities in the source code of the Venus WstETHOracleV2 Upgrade 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.

OVERVIEW | VENUS WSTETHORACLEV2 UPGRADE

This audit concerns the changes made in files outlined in the following PRs:

- [PR-286](#)

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>.

PR-286

This PR updates WstETHOracleV2 to allow a different underlying token than stETH to be specified in the CorrelatedTokenOracle. The underlying amount is still determined by calling `getPooledEthByShares()` in the stETH contract, so that the underlying token must be chosen so that 1 underlying token corresponds to 1 stETH. In particular, this allows the underlying token to be set to WETH, which assumes that 1 stETH is equivalent to 1 WETH.

DEPENDENCIES | VENUS WSTETHORACLEV2 UPGRADE

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:

- stETH

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 increasing fees of third parties, migrating to new LP pools, etc.

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.

FINDINGS | VENUS WSTETHORACLEV2 UPGRADE



3

Total Findings

0

Critical

0

Centralization

0

Major

0

Medium

0

Minor

3

Informational

This report has been prepared to discover issues and vulnerabilities for Venus WstETHOracleV2 Upgrade. 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
VWU-01	<code>underlyingToken</code> Should Be Carefully Configured	Logical Issue	Informational	● Resolved
VWU-02	Typos And Inconsistencies	Inconsistency	Informational	● Resolved
VWU-03	Risks If <code>stETH</code> Market Price Declines Significantly	Design Issue	Informational	● Acknowledged

VWU-01 | `underlyingToken` SHOULD BE CAREFULLY CONFIGURED

Category	Severity	Location	Status
Logical Issue	● Informational	WstETHOracleV2.sol (Base): 22	● Resolved

Description

The `underlyingToken` set in the constructor must be correlated so that 1 `underlyingToken` is equal to 1 stETH. This is because `getUnderlyingAmount()` implicitly assumes this correlation.

Recommendation

We recommend adding checks or clarifying comments in the constructor to ensure that the `underlyingToken` is only set to a token that is safe to assume is 1:1 with stETH.

Alleviation

[CertiK, 06/23/2025]: The team heeded the advice and resolved the issue by adding clarifying comments in commit [dbf8fc5854632b08e187cf76af876926eb20541f](#).

VWU-02 | TYPOS AND INCONSISTENCIES

Category	Severity	Location	Status
Inconsistency	● Informational	WstETHOracleV2.sol (Base): 47~50	● Resolved

Description

The comments above the function `getUnderlyingAmount()` state

```
/**
 * @notice Gets the stETH for 1 wstETH
 * @return amount Amount of stETH
 */
```

However, this function overrides this function from the `CorrelatedTokenOracle`, where the following is

```
/**
 * @notice Gets the underlying amount for correlated token
 * @return underlyingAmount Amount of underlying token
 */
```

If the `underlyingToken` is set to WETH or another underlying token instead of stETH then these are not consistent.

To be consistent it should state that it gets the amount of `underlyingToken` for 1 wstETH assuming that 1 `underlyingToken` is equivalent to 1 stETH and that it returns the amount of `underlyingToken`.

Recommendation

We recommend fixing the typos and inconsistencies mentioned above.

Alleviation

[CertiK, 06/23/2025]: The team heeded the advice and resolved the issue by updating the comments in commit [1d2cd33a7385a35c7ae46cfc08a639eb6f2c26ee](#).

VWU-03 | RISKS IF stETH MARKET PRICE DECLINES SIGNIFICANTLY

Category	Severity	Location	Status
Design Issue	● Informational		● Acknowledged

Description

This update allows 1 stETH to be assumed to be equal to 1 WETH and use the market price of WETH, rather than referencing the market price of stETH through an oracle. Using the market price of stETH as the reference can increase the risk of liquidations if stETH temporarily deviates from its fundamental value, a situation that may occur naturally during ETH price drawdowns. By decoupling liquidation conditions from the market-driven price, the system reduces the potential for liquidation events triggered by short-term price discrepancies.

While this is optimal in most scenarios, there are extreme cases where the market price of stETH may decline significantly below the assumed exchange rate. If this decreases by more than the liquidation threshold, it allows for continuous arbitrage within the protocol. In such a case the market would need to be frozen quickly to avoid severe instability.

Recommendation

We recommend ensuring that users are aware of the tradeoffs associated with these changes and ensure that there are sufficient mitigations in place to handle the more extreme cases.

Alleviation

[Venus, 06/23/2025]: "Issue acknowledged. I won't make any changes for the current version."

We monitor the discrepancy in the USD value of wstETH, assuming and not assuming $1 \text{ stETH} == 1 \text{ ETH}$. We deployed a contract [here](#), not assuming that equivalence, and we compare both prices. If the difference is significant, an alarm is triggered and we'll evaluate the situation, performing the agreed actions depending on the specific scenario."

APPENDIX | VENUS WSTETHORACLEV2 UPGRADE

Finding Categories

Categories	Description
Inconsistency	Inconsistency findings refer to different parts of code that are not consistent or code that does not behave according to its specification.
Logical Issue	Logical Issue findings indicate general implementation issues related to the program logic.
Design Issue	Design Issue findings indicate general issues at the design level beyond program logic that are not covered by other finding categories.

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.

