CERTIK

Venus - WUSDMLiquidator

Security Assessment

CertiK Assessed on Apr 29th, 2025

CertiK Assessed on Apr 29th, 2025

Venus - WUSDMLiquidator

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

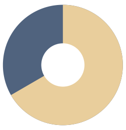
Executive Summary

TYPES	ECOSYSTEM	METHODS
DeFi	zkSync	Manual Review, Static Analysis
LANGUAGE	**TIMELINE**	**KEY COMPONENTS**
Solidity	Delivered on 04/29/2025	N/A

CODEBASE
base
update
View All in Codebase Page

COMMITS
0c7461c10194159d86476812c75eafcec4bf1774
c57bbf0ec66f606ede845a3d7820cffcbecbd410
View All in Codebase Page

Vulnerability Summary



3	3	0	0	0
Total Findings	Resolved	Partially Resolved	Acknowledged	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.
🟨 2	Minor	2 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 | VENUS - WUSDMLIQUIDATOR

CODEBASE | VENUS - WUSDMLIQUIDATOR

Repository

base

update

Commit

0c7461c10194159d86476812c75eafcec4bf1774 c57bbf0ec66f606ede845a3d7820cffcbecbd410

AUDIT SCOPE | VENUS - WUSDMLIQUIDATOR

2 files audited ● 2 files with Resolved findings

ID	Repo	File	SHA256 Checksum
● CSV	VenusProtocol/isolated-pools	contracts/ComptrollerStorage.sol	cc01d538abbe717bdb4465b41da7d4f0cc3f60ef379e1a0542ffd206a46a47dc
● WUS	VenusProtocol/isolated-pools	contracts/WUSDMLiquidator.sol	de2ff0603357d63114975b6c912113bee1cf24d3c65bb922b53d9f47918d554c

APPROACH & METHODS | VENUS - WUSDMLIQUIDATOR

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

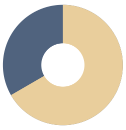
The auditing process pays special attention to the following considerations:

- 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.

FINDINGS | VENUS - WUSDMLIQUIDATOR



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

This report has been prepared to discover issues and vulnerabilities for Venus - WUSDMLiquidator. 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
VEW-01	`run()` Is Unprotected	Access Control	Minor	● Resolved
VEW-02	`_configureMarkets()` Side Effects	Volatile Code	Minor	● Resolved
VEW-03	`closeFactorMantissa` Is Set Via Comptroller Upgrade	Volatile Code	Informational	● Resolved

VEW-01 | `run()` IS UNPROTECTED

Category	Severity	Location	Status
Access Control	● Minor	contracts/WUSDMLiquidator.sol (base): 83	● Resolved

Description

Despite the description stating that the WUSDMLiquidator is meant to be executed solely by Governance, the `run()` function is unprotected and can be called multiple times by any user.

Recommendation

We recommend protecting it with the `onlyOwner` modifier.

Alleviation

[Venus, 04/29/2025]: The team heeded the advice and resolved the issue by protecting the function in commit c57bbf0ec66f606ede845a3d7820cffcbecbd410.

VEW-02 | `_configureMarkets()` SIDE EFFECTS

Category	Severity	Location	Status
Volatile Code	● Minor	contracts/WUSDMLiquidator.sol (base): 111	● Resolved

Description

The `run()` function emits multiple events in the context of the Comptroller and different VTokens on every execution. Since `run()` is unprotected and can be invoked repeatedly, this behavior may lead to unexpected and potentially disruptive events.

Furthermore, the function presumes that the `VWUSDM` market is paused for `Action.MINT` and `Action.ENTER_MARKET`, and maintains the paused state after execution. This may be unintended if the market gets unpaused in the future.

Recommendation

We recommend protecting the `run()` or revoking the access rights of `WUSDMLiquidator` right after the execution.

Alleviation

[Venus, 04/29/2025]: The team heeded the advice and resolved the issue by protecting the function in commit c57bbf0ec66f606ede845a3d7820cffcbecbd410.

VEW-03 | `closeFactorMantissa` IS SET VIA COMPTROLLER UPGRADE

Category	Severity	Location	Status
Volatile Code	● Informational	contracts/ComptrollerStorage.sol (base): 109; contracts/WUSDMLiquidator.sol (base): 124	● Resolved

Description

```
109
    uint256 internal constant MAX_CLOSE_FACTOR_MANTISSA = 1e18; // 1.0, temporarily
```

`WUSDMLiquidator` assumes the Comptroller code will be upgraded, allowing `closeFactorMantissa` to be set higher than the regular 0.9e18. It is unclear when and if the `MAX_CLOSE_FACTOR_MANTISSA` will be restored.

```
124         COMPTROLLER.setCloseFactor(1e18);
```

`WUSDMLiquidator` uses the 1e18 value directly as a close factor. It's reasonable to use `COMPTROLLER.MAX_CLOSE_FACTOR_MANTISSA()` instead to ensure the call will always be successful. Or `MANTISSA_ONE` constant in case it is supposed to revert in case of unexpected COMPTROLLER behavior.

Recommendation

We recommend using `COMPTROLLER.MAX_CLOSE_FACTOR_MANTISSA()` instead and clarifying the timeframe of Comptroller upgraded state.

Alleviation

[Venus, 04/29/2025]: The Comptroller implementation will be upgraded on a Normal VIP, before calling `run()` on the WUSDMLiquidator contract. The original Comptroller implementation will be restored in the same VIP, after the run execution.

APPENDIX | VENUS - WUSDMLIQUIDATOR

Finding Categories

Categories	Description
Access Control	Access Control findings are about security vulnerabilities that make protected assets unsafe.
Volatile Code	Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases and may result in vulnerabilities.

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.