CERTIK

Venus - Token Converter Whitelist Feature

Security Assessment

CertiK Assessed on Aug 11th, 2025

CertiK Assessed on Aug 11th, 2025

Venus - Token Converter Whitelist Feature

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

Executive Summary

TYPES	ECOSYSTEM	METHODS
Lending	Binance Smart Chain (BSC)	Manual Review, Static Analysis

LANGUAGE	TIMELINE	KEY COMPONENTS
Solidity	Delivered on 08/11/2025	N/A

CODEBASE

https://github.com/VenusProtocol/protocol-reserve

View All in Codebase Page

COMMITS

Base: 868c4dc97a15d2b920ea7cecba562c3488ed8ff9

Update1: abc97271b6b81979a2021cbc7bde4a5a7da85dad

View All in Codebase Page

Vulnerability Summary

5 Total Findings	4 Resolved	1 Timelock	0 Partially Resolved	0 Acknowledged	0 Declined

■ 1	Centralization	1 Timelock	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.
■ 1	Minor	1 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.
■ 3	Informational	3 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 - TOKEN CONVERTER WHITELIST FEATURE

CODEBASE | VENUS - TOKEN CONVERTER WHITELIST FEATURE

▌ Repository

https://github.com/VenusProtocol/protocol-reserve

▌ Commit

Base: 868c4dc97a15d2b920ea7cecba562c3488ed8ff9

Update1: abc97271b6b81979a2021cbc7bde4a5a7da85dad

AUDIT SCOPE | VENUS - TOKEN CONVERTER WHITELIST FEATURE

1 file audited ● 1 file without findings

ID	Repo	File	SHA256 Checksum
● STC	VenusProtocol/protocol-reserve	📄 SingleTokenConverter.sol	63907e2cc818e9f8b04a1df844c765e43fe c5c20ad9863f451dd64d34e13f55e

APPROACH & METHODS

VENUS - TOKEN CONVERTER WHITELIST FEATURE

This report has been prepared for Venus to discover issues and vulnerabilities in the source code of the Venus - Token Converter Whitelist Feature 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 - TOKEN CONVERTER WHITELIST FEATURE

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

- PR-146

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-146

This PR is designed to add a new whitelisting mechanism for assets in the `SingleTokenConverter`. The new asset whitelisting mechanism allows designated tokens to be sent directly to the destination address, bypassing the conversion logic. This update introduces an efficient transfer path for select assets while preserving the contract's current features and behaviors.

DEPENDENCIES | VENUS - TOKEN CONVERTER WHITELIST FEATURE

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:

- ERC20 Tokens
- 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 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 - TOKEN CONVERTER WHITELIST FEATURE

5	**0**	**1**	**0**	**0**	**1**	**3**
Total Findings	Critical	Centralization	Major	Medium	Minor	Informational

This report has been prepared to discover issues and vulnerabilities for Venus - Token Converter Whitelist Feature. Through this audit, we have uncovered 5 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
VSW-01	**Centralization Related Risks**	**Centralization**	**Centralization**	● **48h Timelock**
VSW-02	Missing Input Validation	Logical Issue	Minor	● Resolved
VSW-03	Typos And Inconsistencies	Inconsistency	Informational	● Resolved
VSW-04	Missing/Incomplete NatSpec Comments	Inconsistency	Informational	● Resolved
VSW-05	Unchecked Block Can Be Removed	Logical Issue	Informational	● Resolved

VSW-01 | CENTRALIZATION RELATED RISKS

Category	Severity	Location	Status
Centralization	● **Centralization**	**SingleTokenConverter.sol (Base): 80**	● **48h Timelock**

▌ Description

Note that any centralization risks present in the existing codebase before the PR's in scope of this audit were not considered. Only those added to the in-scope PRs are addressed. 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.

In the contract `SingleTokenConverter` , the role `DEFAULT_ADMIN_ROLE` of the `AccessControlManager` can grant addresses the privilege to call the function `setAssetsDirectTransfer()` . Any compromise to the `DEFAULT_ADMIN_ROLE` or accounts granted this privilege may allow the hacker to take advantage of this authority and set an asset for direct transfer so that it is directly transferred to the destination address and is not available for conversion.

▌ Recommendation

The risk describes the current project design and potentially makes iterations to improve in the security operation and level of decentralization, which in most cases cannot be resolved entirely at the present stage. We advise the client to carefully manage the privileged account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., multisignature wallets.

Indicatively, here are some feasible suggestions that would also mitigate the potential risk at a different level in terms of short-term, long-term and permanent:

Short Term:

Timelock and Multi sign (⅔, ⅗) combination *mitigate* by delaying the sensitive operation and avoiding a single point of key management failure.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
  AND
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key compromised;
  AND
- A medium/blog link for sharing the timelock contract and multi-signers addresses information with the public audience.

Long Term:

Timelock and DAO, the combination, *mitigate* by applying decentralization and transparency.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;

  AND

- Introduction of a DAO/governance/voting module to increase transparency and user involvement.

  AND

- A medium/blog link for sharing the timelock contract, multi-signers addresses, and DAO information with the public audience.

Permanent:

Renouncing the ownership or removing the function can be considered *fully resolved*.

- Renounce the ownership and never claim back the privileged roles.

  OR

- Remove the risky functionality.

Alleviation

[Venus, 08/11/2025]: We'll use the AccessControlManager (ACM) already deployed (see addresses here: https://docs-v4.venus.io/deployed-contracts/governance).

In these ACM, only the Normal Timelock (i.e. 0x939bd8d64c0a9583a7dcea9933f7b21697ab6396 on BNB Chain) has the DEFAULT_ADMIN_ROLE. And this contract is a Timelock contract used during the Venus Improvement Proposals.

We'll authorize Normal, Fast-track and Critical Timelocks to execute the mentioned function.

The current config for the three Timelock contracts are:

- normal: 24 hours voting + 48 hours delay
- fast-track: 24 hours voting + 6 hours delay
- critical: 6 hours voting + 1 hour delay

VSW-02 | MISSING INPUT VALIDATION

Category	Severity	Location	Status
Logical Issue	● Minor	SingleTokenConverter.sol (Base): 137, 145	● Resolved

Description

The `_setAssetsDirectTransfer()` function lacks input validation in two key areas. First, it does not verify whether the new value assigned to `assetsDirectTransfer[assets[i]]` differs from its current value. Updating the mapping with an identical value is redundant and could signal a mistake in the provided inputs. Second, the function does not prevent the `baseAsset` from being included in the assets array. If the `baseAsset` is set as an asset for direct transfer, and later updated via `setBaseAsset()`, the original base asset will continue to be directly transferred without conversion. This behavior may cause confusion or introduce inconsistencies in the asset conversion process.

Recommendation

We recommend adding the input validations mentioned above.

Alleviation

[CertiK, 08/11/2025]: The client made the recommended changes resolving this finding in commit abc97271b6b81979a2021cbc7bde4a5a7da85dad.

VSW-03 | TYPOS AND INCONSISTENCIES

Category	Severity	Location	Status
Inconsistency	● Informational	SingleTokenConverter.sol (Base): 75, 91~95	● Resolved

Description

In the comments above the function `setAssetsDirectTransfer()` it states "assets Addresses of the assets need to be added for direct transfer". However, these are assets that are either added **or removed** for direct transfer.

In the comments above the function `_setAssetsDirectTransfer` it states "assets Addresses of the assets need to be added for direct transfer". However, these are assets that are either added **or removed** for direct transfer.

The comments above the function `_updateAssetsState()` do not describe the behavior that if the input asset is the base asset or has the `assetsDirectTransfer` mapping set to true, that it will transfer the tokens directly to the `destinationAddress` and not hold them for conversion.

Recommendation

We recommend fixing the typos and inconsistencies mentioned above.

Alleviation

[CertiK, 08/11/2025]: The client made the recommended changes resolving this finding in commit 416d0259c7ef34e5cddacdd006e338bcd62ba0dc.

VSW-04 | MISSING/INCOMPLETE NATSPEC COMMENTS

Category	Severity	Location	Status
Inconsistency	● Informational	SingleTokenConverter.sol (Base): 67~69, 73~78	● Resolved

Description

The NatSpec comments for the function `setAssetsDirectTransfer()` do not document the possible `InputLengthMisMatch` error that can occur. The NatSpec comments for the function `setBaseAsset` do not document the possible events or errors it may emit.

Recommendation

We recommend fixing the NatSpec comments mentioned above.

Alleviation

[CertiK, 08/11/2025]: The client made the recommended changes resolving this finding in commit 18bd5394e3599e9af0af162b402b96567a02fb5a.

VSW-05 | UNCHECKED BLOCK CAN BE REMOVED

Category	Severity	Location	Status
Logical Issue	● Informational	SingleTokenConverter.sol (Base): 147~149	● Resolved

Description

Due to the improvements introduced in Solidity version 0.8.22, the use of an explicit `unchecked` block for incrementing loop counters is now redundant, as the compiler automatically applies the relevant optimizations where applicable. The original for loop structure, without the `unchecked` block, is sufficient and improves code readability.

Recommendation

We recommend removing unnecessary unchecked blocks around loop counter increments and using the original for loop structure.

Alleviation

[CertiK, 08/11/2025]: The client made the recommended changes resolving this finding in commit d3bcf379b3f16e912fd2bb01004870d65f80beca.

APPENDIX | VENUS - TOKEN CONVERTER WHITELIST FEATURE

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.
Centralization	Centralization findings detail the design choices of designating privileged roles or other centralized controls over the code.

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.