CERTIK

Venus - Forced liquidations in Isolated pools

CertiK Assessed on Oct 16th, 2023

CertiK Assessed on Oct 16th, 2023

Venus - Forced liquidations in Isolated pools

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 10/16/2023	N/A

CODEBASE

isolated-pools

View All in Codebase Page

COMMITS

base: cbd9b18a99c4e1f92bf9404e88fceb8ebc36d55f

Update 1: ebc9a9b043064e6fe4af2ac48fdc24e24eddba58

View All in Codebase Page

Vulnerability Summary

5 Total Findings	2 Resolved	2 Mitigated	0 Partially Resolved	1 Acknowledged	0 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.
■ 2	Major	2 Mitigated	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.
■ 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 - FORCED LIQUIDATIONS IN ISOLATED POOLS

CODEBASE | VENUS - FORCED LIQUIDATIONS IN ISOLATED POOLS

▌ Repository

isolated-pools

▌ Commit

base: cbd9b18a99c4e1f92bf9404e88fceb8ebc36d55f

Update 1: ebc9a9b043064e6fe4af2ac48fdc24e24eddba58

AUDIT SCOPE

VENUS - FORCED LIQUIDATIONS IN ISOLATED POOLS

2 files audited ● 2 files without findings

ID	File	SHA256 Checksum
● CVP	Comptroller.sol	8649b50cdfcbc1a0a2f336833c35facce17cfc013f3500947081cb0187d465ff
● CSV	ComptrollerStorage.sol	9637ede2563ac85c66c2f908519d5c4c73b3762a6b61dfc229c41add4d7a722d

APPROACH & METHODS

VENUS - FORCED LIQUIDATIONS IN ISOLATED POOLS

This report has been prepared for Venus to discover issues and vulnerabilities in the source code of the Venus - Forced liquidations in Isolated pools 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.

PROJECT SUMMARY

VENUS - FORCED LIQUIDATIONS IN ISOLATED POOLS

This audit concerns the changes made in files outlined in PR 305, https://github.com/VenusProtocol/isolated-pools/pull/305/, up to commit cbd9b18a99c4e1f92bf9404e88fceb8ebc36d55f.

The PR added the ability to force liquidations for certain markets, replacing the `isDeprecated()` terminology to be more consistent throughout all pools.

This was done by adding a mapping `isForcedLiquidationEnabled` from markets to a bool indicating if they are able to be force liquidated. This mapping is set via the newly added function `setForcedLiquidation()`, which is restricted by the access control manager. The mapping is used in the `preLiquidateHook` function, to skip checking the shortfall and close limit checks. If force liquidation is enabled for a market, it allows the full amount of any borrow from that market to be liquidated, regardless of its collateral factor and close factor.

FINDINGS | VENUS - FORCED LIQUIDATIONS IN ISOLATED POOLS

5 Total Findings	**0** Critical	**2** Major	**0** Medium	**0** Minor	**3** Informational

This report has been prepared to discover issues and vulnerabilities for Venus - Forced liquidations in Isolated pools. 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
CVP-01	**Centralized Control Of Contract Upgrade**	**Centralization**	**Major**	● **Mitigated**
CVP-02	**Centralization Related Risks**	**Centralization**	**Major**	● **Mitigated**
CVP-03	Inconsistencies	Inconsistency	Informational	● Resolved
CVP-04	Unnecessary `address` Casting	Code Optimization	Informational	● Resolved
CVP-05	Potential Rate Manipulation If Force Liquidated Markets Are Reenabled	Logical Issue	Informational	● Acknowledged

CVP-01 | CENTRALIZED CONTROL OF CONTRACT UPGRADE

Category	Severity	Location		Status
Centralization	● **Major**	**Comptroller.sol (Comptroller-Base): 39**		● **Mitigated**

Description

In the contract `Comptroller` , the proxy `admin` has the authority to update the implementation contract behind the contract.

Any compromise to the `admin` account may allow a hacker to take advantage of this authority and change the implementation contract, which is pointed by proxy, and therefore execute potential malicious functionality in the implementation contract.

Recommendation

We recommend that the team make efforts to restrict access to the admin of the proxy contract. A strategy of combining a time-lock and a multi-signature (⅔, ⅗) wallet can be used to prevent a single point of failure due to a private key compromise. In addition, the team should be transparent and notify the community in advance whenever they plan to migrate to a new implementation contract.

Here are some feasible short-term and long-term suggestions that would mitigate the potential risk to a different level and suggestions that would permanently fully resolve the risk.

Short Term:

A combination of a time-lock and a multi signature (⅔, ⅗) wallet mitigate the risk by delaying the sensitive operation and avoiding a single point of key management failure.

- A time-lock with reasonable latency, such as 48 hours, for awareness of privileged operations;
  AND
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to a private key compromised;
  AND
- A medium/blog link for sharing the time-lock contract and multi-signers addresses information with the community.

For remediation and mitigated status, please provide the following information:

- Provide the deployed time-lock address.

- Provide the **gnosis** address with **ALL** the multi-signer addresses for the verification process.

- Provide a link to the **medium/blog** with all of the above information included.

Long Term:

A combination of a time-lock on the contract upgrade operation and a DAO for controlling the upgrade operation mitigate the contract upgrade risk by applying transparency and decentralization.

- A time-lock with reasonable latency, such as 48 hours, for community awareness of privileged operations;
  AND
- Introduction of a DAO, governance, or voting module to increase decentralization, transparency, and user involvement;
  AND
- A medium/blog link for sharing the time-lock contract, multi-signers addresses, and DAO information with the community.

For remediation and mitigated status, please provide the following information:

- Provide the deployed time-lock address.

- Provide the **gnosis** address with **ALL** the multi-signer addresses for the verification process.

- Provide a link to the **medium/blog** with all of the above information included.

Permanent:

Renouncing ownership of the `admin` account or removing the upgrade functionality can *fully* resolve the risk.

- Renounce the ownership and never claim back the privileged role;
  OR
- Remove the risky functionality.

Alleviation

`[Venus, 10/12/2023]` : Comptrollers in Isolated pools use a Beacon proxy. The Beacon proxy is deployed at 0x38B4Efab9ea1bAcD19dC81f19c4D1C2F9DeAe1B2. The owner of this Beacon proxy is 0x939bd8d64c0a9583a7dcea9933f7b21697ab6396, the Normal Timelock used to execute the normal Venus Improvement Proposals (VIP). For normal VIPs, the time config is: 24 hours voting + 48 hours delay before the execution.

Only the owner of the Beacon proxy can invoke the function upgradeTo, so, the Comptroller in Isolated pools will be upgraded only via a Normal VIP, involving the community in the process.

CVP-02 | CENTRALIZATION RELATED RISKS

Category	Severity	Location	Status
Centralization	● **Major**	**Comptroller.sol (Comptroller-Base): 1016~1017**	● **Mitigated**

▌ Description

The centralization risks indicated here are only related to those within the scope of the delta audit. CertiK has audited the `isolated-pools` repository and more information regarding the centralization risks can be found in our previous audits:https://skynet.certik.com/projects/venus.

Comptroller

The role `DEFAULT_ADMIN_ROLE` can grant addresses the privilege to call the following functions:

- `setForcedLiquidation()`

Any compromise to the `DEFAULT_ADMIN_ROLE` or these privileged functions may allow the hacker to take advantage of this authority and do the following:

- Enable forced liquidation on any market, allowing all borrows to be liquidated. This will cause users who have healthy borrows to still be liquidated and subject them to the liquidation fee. If this is executed unexpectedly, users may not have adequate time to repay their borrows in order to avoid being subject to liquidation fees.

▌ 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, 10/12/23]` : Regarding the DEFAULT_ADMIN_ROLE, we'll use the AccessControlManager (ACM) deployed at 0x4788629abc6cfca10f9f969efdeaa1cf70c23555. In this ACM, only 0x939bd8d64c0a9583a7dcea9933f7b21697ab6396 (Normal Timelock) has the DEFAULT_ADMIN_ROLE. And this contract is a Timelock contract used during the Venus Improvement Proposals.

We'll allow Normal, Fast-track [a] and Critical [b] timelock contracts to execute the function setForcedLiquidation().

Specifically, 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

[a] 0x555ba73dB1b006F3f2C7dB7126d6e4343aDBce02

[b] 0x213c446ec11e45b15a6E29C1C1b402B8897f606d

CVP-03 | INCONSISTENCIES

Category	Severity	Location	Status
Inconsistency	● Informational	Comptroller.sol (Comptroller-Base): 480, 1016	● Resolved

Description

The comment above the force liquidation check states: "Allow accounts to be liquidated if the market is deprecated or it is a forced liquidation". However, there are no checks allowing a market to be liquidated if it is deprecated.

In addition, it should be ensured that a market is deprecated before forced liquidations are enabled. Otherwise, users may accidentally open positions can be immediately liquidated.

Recommendation

We recommend fixing the inconsistency in the comment and ensuring through markets are deprecated before enabling force liquidations. This can be done by the project team before calling `setForcedLiquidation()` or checks for the appropriate parameters can be included in the function `setForcedLiquidation()`.

Alleviation

`[CertiK, 10/13/2023]` : The team made changes resolving the finding in commit ebc9a9b043064e6fe4af2ac48fdc24e24eddba58.

They further state the following:

`[Venus, 10/13/2023]` : "setForcedLiquidation() will be invoked in a VIP, so there will be a process where the community will be able to check that the market is "deprecated" (usually with the borrow and supply actions paused)"

CVP-04 | UNNECESSARY `address` CASTING

Category	Severity	Location	Status
Code Optimization	● Informational	Comptroller.sol (Comptroller-Base): 1024~1025	● Resolved

▌ Description

Input `vTokenBorrowed` in function `setForcedLiquidation()` is already `address` type; using the `address` casting on the input before using it as a key in `isForcedLiquidationEnabled` is unnecessary.

▌ Recommendation

We recommend removing the `address` casting on `vTokenBorrowed` when used in `isForcedLiquidationEnabled`.

▌ Alleviation

`[CertiK, 10/13/2023]` : The team made changes resolving the finding in commit
f4e8d2b5517ad6b104cffcdbe03c9eb2fd94ddbc.

CVP-05 | POTENTIAL RATE MANIPULATION IF FORCE LIQUIDATED MARKETS ARE REENABLED

Category	Severity	Location	Status
Logical Issue	● Informational	Comptroller.sol (Comptroller-Base): 1016	● Acknowledged

Description

Tokens should be provided and locked in every market during normal operating conditions, to avoid the total supply becoming low enough that the rate can be significantly manipulated. For example this was the cause of the Hundred Finance Exploit: https://decrypt.co/136918/hacker-exploits-hundred-finance-protocol-in-7-4-million-heist/.

However, when forced liquidations are enabled for markets, it is likely that the total supply of the markets will drop and the project may wish to redeem their locked tokens. If all operations are frozen for the market, then redeeming the locked tokens can be executed safely. However, if in the future the market is to be enabled and supported again, it must be ensured that tokens are supplied and locked in the market in the same transaction that operations are unfrozen.

Recommendation

We recommend either leaving an amount of the token locked to ensure that such a rate manipulation is non-profitable or to ensure that tokens are resupplied and locked atomically, when a market is reenabled after it has been frozen and forced liquidated.

Alleviation

[Venus, 10/13/2023] : Issue acknowledged. I won't make any changes for the current version.

If the market is reenabled, it will be done via VIP, so there will be a period of time to review it. Moreover, we are aware of the Hundred Finance Exploit, and we consider it in our risk evaluations.

APPENDIX | VENUS - FORCED LIQUIDATIONS IN ISOLATED POOLS

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.

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.