



Security Assessment

# Venus - Force Liquidations

CertiK Assessed on Sept 16th, 2023





CertiK Assessed on Sept 16th, 2023

## Venus - Force Liquidations

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

### Executive Summary

#### TYPES

DeFi

#### ECOSYSTEM

Binance Smart Chain  
(BSC)

#### METHODS

Manual Review, Static Analysis

#### LANGUAGE

Solidity

#### TIMELINE

Delivered on 09/16/2023

#### KEY COMPONENTS

N/A

#### CODEBASE

<https://github.com/VenusProtocol/venus-protocol>

View All in Codebase Page

#### COMMITTS

base: [eaf564f93e9f088eef208ba69bd26d438447fc96](#)

View All in Codebase Page

### Vulnerability Summary



2

Total Findings

0

Resolved

1

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.

1 Major

1 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.

1 Informational

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 - FORCE LIQUIDATIONS

## **I Summary**

Executive Summary

Vulnerability Summary

Codebase

Audit Scope

Approach & Methods

## **I Summary**

## **I Findings**

CCV-01 : Centralization Related Risks

CCV-02 : Potential Rate Manipulation If Force Liquidated Markets Are Reenabled

## **I Appendix**

## **I Disclaimer**

# CODEBASE | VENUS - FORCE LIQUIDATIONS

## Repository



<https://github.com/VenusProtocol/venus-protocol>

## Commit

base: [eaf564f93e9f088eef208ba69bd26d438447fc96](#)

## AUDIT SCOPE | VENUS - FORCE LIQUIDATIONS

2 files audited ● 2 files without findings

| ID    | Repo                         | File   | SHA256 Checksum  |
|-------|------------------------------|--|--|
| ● CCV | VenusProtocol/venus-protocol |  Comptroller.sol        | 6355aecd2670add8d0954d82e130714bbc<br>b8ed58033d5482badb98a228a16b79 |
| ● CSC | VenusProtocol/venus-protocol |  ComptrollerStorage.sol | b445e8ec1d738526776a6391f5d40b3e67<br>ec7c379e58ad8d54b5fd1b1d7ae5cd |

## APPROACH & METHODS | VENUS - FORCE LIQUIDATIONS

This report has been prepared for Venus to discover issues and vulnerabilities in the source code of the Venus - Force Liquidations 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 - FORCE LIQUIDATIONS

This audit concerns the changes made in files outlined in PR 332, <https://github.com/VenusProtocol/venus-protocol/pull/332>, up to commit [eaf564f93e9f088eef208ba69bd26d438447fc96](#).

The PR added the ability to force liquidations for certain markets and bytecode optimizations to allow the additional functionality to be added without exceeding the contract size limit.

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 `liquidateBorrowAllowed` hook, 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 - FORCE LIQUIDATIONS



2

Total Findings

0

Critical

1

Major

0

Medium

0

Minor

1

Informational

This report has been prepared to discover issues and vulnerabilities for Venus - Force Liquidations. Through this audit, we have uncovered 2 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         |
|--------|---|----------------|---------------|----------------|
| CCV-01 | Centralization Related Risks  | Centralization | Major         | ● Mitigated    |
| CCV-02 | Potential Rate Manipulation If Force Liquidated Markets Are Reenabled | Logical Issue  | Informational | ● Acknowledged |



## CCV-01 | CENTRALIZATION RELATED RISKS

| Category       | Severity | Location                       | Status      |
|----------------|----------|--------------------------------|-------------|
| Centralization | ● Major  | Comptroller.sol (newBase): 926 | ● Mitigated |

### Description

The centralization risks indicated here are only related to those within the scope of the audit. CertiK has not audited the whole `venus-protocol` repository before and we recommend users to carefully review the handling of privileged roles throughout the codebase.

### 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 force 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 the 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 (2/3, 3/5) 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.

### I Alleviation

[Venus, 09/08/2023] : 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 and Critical timelock contracts to execute the function `setForcedLiquidation()`.

[Certik, 09/08/2023] : The client has adopted the timelock and dao long-term solution, so we mark this finding as *mitigated*. While this strategy has indeed reduced the risk, it's crucial to note that it has not completely eliminated it.

## CCV-02 | POTENTIAL RATE MANIPULATION IF FORCE LIQUIDATED MARKETS ARE REENABLED

| Category      | Severity        | Location                           | Status         |
|---------------|-----------------|------------------------------------|----------------|
| Logical Issue | ● Informational | Comptroller.sol (newBase): 551~556 | ● 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, 09/08/2023] : 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 - FORCE LIQUIDATIONS

### Finding Categories

| Categories     | Description  |
|----------------|--|
| 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.

