



Security Assessment

# Venus - Two Kinks Interest Rate

CertiK Assessed on Jul 31st, 2024





CertiK Assessed on Jul 31st, 2024

## Venus - Two Kinks Interest Rate

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 07/31/2024

#### KEY COMPONENTS

N/A

#### CODEBASE

PR-494: <https://github.com/VenusProtocol/venus-protocol/pull/494>PR-417: <https://github.com/VenusProtocol/isolated-pools/pull/417>[View All in Codebase Page](#)

#### COMMITTS

PR-494-Base: [e9aee5ce51795cc4ec35588bb9af3190070f8746](https://github.com/VenusProtocol/venus-protocol/pull/494)PR-417-Base: [5a93f4d1b4d23d93b33b027f3aa72bd47e05d987](https://github.com/VenusProtocol/isolated-pools/pull/417)PR-494-Update1: [4c9be09cc591e9f1eff5a596e699d380340c8073](https://github.com/VenusProtocol/venus-protocol/pull/494)[View All in Codebase Page](#)

### Vulnerability Summary



4

Total Findings

3

Resolved

0

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.

0 Major

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.

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

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 - TWO KINKS INTEREST RATE

## **I Summary**

[Executive Summary](#)

[Vulnerability Summary](#)

[Codebase](#)

[Audit Scope](#)

[Approach & Methods](#)

## **I Summary**

## **I Findings**

[VPB-03 : Missing Checks](#)

[VPB-01 : `\\_max\(\)` Inconsistencies](#)

[VPB-04 : Inconsistency With Provided Documentation](#)

[VPB-05 : Typos And Inconsistencies](#)

## **I Optimizations**

[VPB-02 : Unchecked Blocks Can Optimize Contract](#)

## **I Appendix**

## **I Disclaimer**

# CODEBASE | VENUS - TWO KINKS INTEREST RATE

## Repository

PR-494: <https://github.com/VenusProtocol/venus-protocol/pull/494>

PR-417: <https://github.com/VenusProtocol/isolated-pools/pull/417>

## Commit

PR-494-Base: [e9aee5ce51795cc4ec35588bb9af3190070f8746](#)

PR-417-Base: [5a93f4d1b4d23d93b33b027f3aa72bd47e05d987](#)

PR-494-Update1: [4c9be09cc591e9f1eff5a596e699d380340c8073](#)




PR-417-Update1: [455533e0eb2213fc8ec29a983389868e25f42038](#)

PR-494-Update2: [72133a8b164f7f2f78bd4d795f5460f891c74c78](#)

PR-417-Update2: [37ffc7963b209a61d2afc92bd061398268f163ae](#)

## AUDIT SCOPE | VENUS - TWO KINKS INTEREST RATE

3 files audited ● 2 files with Acknowledged findings ● 1 file without findings

ID	Repo	File	SHA256 Checksum
● TKI	VenusProtocol/isolated-pools	 contracts/TwoKinksInterestRateModel.sol	de2522e0b2a62695fcd4a5a36f7818a56d73921fbd629e651e33ced9b3b9e70f
● TKR	VenusProtocol/venus-protocol	 contracts/InterestRateModels/TwoKinksInterestRateModel.sol	477232895918fd9156cc900566d9a1e491849e03bf6c73b6c7608ac63720c244
● IRM	VenusProtocol/venus-protocol	 contracts/InterestRateModels/InterestRateModelV8.sol	10512d8de8cf1aab5db5c8fd16cfd13d119b64e6f0fd110efeafa22c222df84a

## APPROACH & METHODS | VENUS - TWO KINKS INTEREST RATE

This report has been prepared for Venus to discover issues and vulnerabilities in the source code of the Venus - Two Kinks Interest Rate 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 - TWO KINKS INTEREST RATE

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

- [Isolated Pools PR-417](#)
- [Venus Protocol PR-494](#)

Note that any centralization risks present in the existing codebase before these PRs were not considered in this audit. We recommend all users to 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 particular, these PRs are designed to include a new two kink interest rate model, which is similar to the jump rate model. The difference being that the jump rate model uses a single kink, while the two kink interest rate model utilizes two kinks. The borrow and thus the supply rate are determined by functions depending on the utilization rate. The borrow rate of the two kink model is a piecewise linear function, where two utilization rates `kink1` and `kink2` give the boundary points. This allows the borrow and thus the supply rate curves to have differing linear functions for three ranges of utilization rates and can allow for separate linear functions for low, medium, and high utilization rates. In addition, the implementation allows for negative slopes in the piecewise functions, which allows for borrow rates to decrease while the utilization rate increases.

In general, the effectiveness of this model depends on inputs being carefully selected for the market in which it is used. This is outside the scope of this audit and only the correctness of the implementation was considered during the audit.

## FINDINGS | VENUS - TWO KINKS INTEREST RATE



4

Total Findings

0

Critical

0

Major

0

Medium

1

Minor

3

Informational

This report has been prepared to discover issues and vulnerabilities for Venus - Two Kinks Interest Rate. Through this audit, we have uncovered 4 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
VPB-03	Missing Checks	Logical Issue	Minor	● Resolved
VPB-01	<code>_max()</code> Inconsistencies	Logical Issue	Informational	● Resolved
VPB-04	Inconsistency With Provided Documentation	Logical Issue	Informational	● Acknowledged
VPB-05	Typos And Inconsistencies	Inconsistency	Informational	● Resolved



## VPB-03 | MISSING CHECKS

Category	Severity	Location	Status
Logical Issue	Minor	contracts/TwoKinksInterestRateModel.sol (PR-417-Base): 75, 78, 83; contracts/InterestRateModels/TwoKinksInterestRateModel.sol (PR-494-Base): 76, 79, 82	Resolved

### Description

The `constructor()` does not perform the following checks:

- It does not check that `kink1_ < kink2_`. If `kink2_` is less than `kink1_` the curve will not have the desired shape.
- It does not check that `kink1` is strictly greater than 0. This should be done if the intention is to always have three linear functions. If the intention is to allow two, we recommend considering creating a separate contract to handle this.

### Recommendation

We recommend adding the checks mentioned above.

### Alleviation

[Certik, 07/31/2024]: The client made changes resolving the finding in commits

- [f339105dbce91c202beed6d6a14fcf75efb29058](#);
- [ece33796e826a15b70df06a5a1d2385e80feaa92](#);
- [72133a8b164f7f2f78bd4d795f5460f891c74c78](#);
- [37ffc7963b209a61d2afc92bd061398268f163ae](#).

## VPB-01 | `_max()` INCONSISTENCIES

Category	Severity	Location	Status
Logical Issue	● Informational	contracts/TwoKinksInterestRateModel.sol (PR-417-Base): 207~209; contracts/InterestRateModels/TwoKinksInterestRateModel.sol (PR-494-Base): 181~183	● Resolved

### Description

The function `_max()` takes two `int256` as input and returns the larger of the two numbers. However, if they are both negative, then it will cast the greater negative number to a `uint256` causing it to return a large value.

This function is only used internally and one of the inputs is always zero, so that these cases are not relevant to the current contract. However, if this function is adapted to be used in the future, then these cases may need to be considered and handled.

### Recommendation

We recommend refactoring the function to take a single input as in all cases the first input is zero.

### Alleviation

[Certik, 07/30/2024]: The client made the recommended changes in commits

- [455533e0eb2213fc8ec29a983389868e25f42038](#);
- [4c9be09cc591e9f1eff5a596e699d380340c8073](#).

## VPB-04 | INCONSISTENCY WITH PROVIDED DOCUMENTATION

Category	Severity	Location	Status
Logical Issue	● Informational	contracts/TwoKinksInterestRateModel.sol (PR-417-Base): 74, 76, 79; contracts/InterestRateModels/TwoKinksInterestRateModel.sol (PR-494-Base): 75, 77, 80	● Acknowledged

### Description

The two kink interest rate model gets the borrow rate as a piecewise linear function whose boundary points are given by `kink1` and `kink2`.

The provided documentation provided two models, one of which only included linear curves with positive slope, and the second that only allowed for a linear curve with negative slope between `kink1` and `kink2`.

However, the implementation makes no checks on any of the multipliers, so that all three linear curves of the piecewise function are allowed to have negative slope.

While it may be desired to have negative slope linear curves in the intervals `[0, kink1]` and `[kink1, kink2]`, the interval `[kink2, 1e18]` has the highest utilization rates and should incentivize users to payback their borrows by having a higher borrow rate. As such the slope for the linear function in this interval should be positive to increase the borrow rates as the utilization rate closely approaches 100 percent.

In addition, the utilization of negative multipliers requires the addition of some checks and castings which increase gas costs slightly. As such it may be beneficial to create two separate rate models as in the documentation. One that only allows for positive multipliers and the other which allows for desired negative multipliers.

Last, it should be noted that in the case where `max(0, output)` is 0, where `output` represents one of three formulae depending on the subinterval, this may present an extra kink in the interest rate model, via a horizontal slope, until the `output` value is again positive. In this way, there may be more than two kinks in the interest rate model.

### Recommendation

We recommend determining which intervals you will allow negative multipliers for and enforcing this when they are set in the constructor. In addition, we recommend considering creating two separate rate models, one for only positive multipliers, and the other allowing negative multipliers.

### Alleviation

[Venus, 07/30/2024] : "Issue acknowledged. I won't make any changes for the current version."

We will maintain only one contract (to simplify the management of the codebase), allowing negative slopes at every interval. The mentioned constraints (i.e. to keep a positive slope always in the last interval) would be a business decision, taken and

considered during the configuration and review of the VIP."

## VPB-05 | TYPOS AND INCONSISTENCIES

Category	Severity	Location	Status
Inconsistency	● Informational	contracts/TwoKinksInterestRateModel.sol (PR-417-Base): 11, 5 1, 63, 65, 66, 103; contracts/InterestRateModels/TwoKinksInterestRateModel.sol (PR-494-Base): 9, 51, 66, 68, 69, 100	● Resolved

### Description

The comment at the start of the `TwoKinksInterestRateModel` contracts state "An interest rate model with two different steep increase each after a certain utilization threshold called **kink** is reached."

However, the implementation does not just allow for steep increases, in general the implementation allows for the slope to be increased or decreased when each kink is reached.

The comment above `getBorrowRate()` states that the return value is "scaled by 1e18" when all other comments instead use "scaled by EXP\_SCALE"

The comment above `JUMP_MULTIPLIER_PER_BLOCK` is not consistent with the comments for the `MULTIPLIER_2_PER_BLOCK` or `MULTIPLIER_PER_BLOCK`. It could be reworded to be "The multiplier of utilization rate per block that gives the slope 3 of the interest rate".

The comments for the inputs `multiplierPerYear_` and `multiplier2PerYear_` in the `constructor()` state "The rate of increase". However, with the current implementation these can be negative values so that it can be the rate of increase or decrease.

The comment for the input `baseRate2PerYear_` in the `constructor` states "The approximate target base APR after hitting `KINK_1`, as a mantissa (scaled by EXP\_SCALE)". However the `baseRate2PerYear_` value represents a discontinuous increase in APR, as the calculation of the rate adds the rate from the previous interval.

### Recommendation

We recommend fixing the typos and inconsistencies mentioned above.

### Alleviation

[Certik, 07/26/2024]: The client made the recommended changes in commits

- [b5df8d29db3e3d9e86ac01e82b5c3ab39b9222e4](#);

- [dd52dc9e40ddd60af5246a0eb65c52cbf27ce7fd](#).

## OPTIMIZATIONS | VENUS - TWO KINKS INTEREST RATE

ID	Title	Category	Severity	Status
<u>VPB-02</u>	Unchecked Blocks Can Optimize Contract	Gas Optimization	Optimization	● Resolved

## VPB-02 | UNCHECKED BLOCKS CAN OPTIMIZE CONTRACT

Category	Severity	Location	Status
Gas Optimization	● Optimization	contracts/TwoKinksInterestRateModel.sol (PR-417-Base): 187, 193, 195; contracts/InterestRateModels/TwoKinksInterestRateModel.sol (PR-494-Base): 163, 168, 169	● Resolved

### Description

In the function `_getBorrowRate()` the calculations `util - KINK_1` and `util - KINK_2` can be placed in unchecked blocks to save gas. This is because `util` is the output of the call to `utilizationRate` so that it will always be in the interval  $[0, 1e18]$ . Then `util - KINK_1` is only executed if `util >= KINK_1` so that it cannot underflow. Similarly `util - KINK_2` is only executed if `util >= KINK_2` so that it cannot underflow.

If the suggested check is made to ensure that `KINK_1 < KINK_2`, then in addition `KINK_2 - KINK_1` can also be placed in an unchecked block.

### Recommendation

We recommend placing the operations that cannot underflow in unchecked blocks to reduce gas costs.

### Alleviation

[Certik, 07/30/2024]: The client made the recommended changes in commits

- [00fdcdbbe86608a8c8d4783a4818c0c94e2c7bf8](#);
- [414bd7d71eac5ce5eefd16ffcb5971c08c20f75e](#).



## APPENDIX | VENUS - TWO KINKS INTEREST RATE

### Finding Categories

Categories	Description
Gas Optimization	Gas Optimization findings do not affect the functionality of the code but generate different, more optimal EVM opcodes resulting in a reduction on the total gas cost of a transaction.
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.

### 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.

