



Security Assessment

Venus - Native Token Gateway

CertiK Assessed on Feb 26th, 2024





Certik Assessed on Feb 26th, 2024

Venus - Native Token Gateway

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

Executive Summary

TYPES

DeFi

ECOSYSTEM

Ethereum (ETH)

METHODS

Manual Review, Static Analysis

LANGUAGE

Solidity

TIMELINE

Delivered on 02/26/2024

KEY COMPONENTS

N/A

CODEBASE

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

View All in Codebase Page

COMMITTS

PR361-Base: [8fb63cc391e405875984aba45debc493d70d652f](#)PR442-Base: [e44d832deb2e6aea87e977d761ef0a648fe7aebb](#)PR361-Update1: [ae0b770a624d0d525968e11c2ebab4aa546ae1a8](#)

View All in Codebase Page

Vulnerability Summary



8

Total Findings

7

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.



1 Major

1 Acknowledged



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.



2 Medium

2 Resolved



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.



5 Informational

5 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 - NATIVE TOKEN GATEWAY

I Summary

Executive Summary

Vulnerability Summary

Codebase

Audit Scope

Approach & Methods

I Summary

Overview

I Dependencies

Third Party Dependencies

Recommendations

I Findings

NTG-04 : Centralization Related Risks

NTG-01 : Lack Of Input Validation

VBV-01 : Extra Approval Will Be Given For Those That Have Already Approved Delegates

NTG-05 : `approve` return value not checked

NTG-06 : Inconsistent Handling Of Wrapped Native Functionality

NTG-07 : Unnecessary `payable` Casting

NTV-01 : Removal Of `fallback()` Assumes `wNativeToken.withdraw()` Will Have Empty `msg.data` When Sending Native Token

VPB-01 : Typos and Inconsistencies

I Appendix

I Disclaimer

CODEBASE | VENUS - NATIVE TOKEN GATEWAY

Repository

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

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

Commit

PR361-Base: [8fb63cc391e405875984aba45debc493d70d652f](#)

PR442-Base: [e44d832deb2e6aea87e977d761ef0a648fe7aebb](#)

PR361-Update1: [ae0b770a624d0d525968e11c2ebab4aa546ae1a8](#)











PR442-Update1: [becfe891329b8c93f46e968051721848d6d05253](#)

PR361-Update2: [eed3a61c0700ae960e63453b68af947248aabc0d](#)

PR442-Update2: [dbd4edcd43bee1a80b57fe034259653eef158e92](#)

AUDIT SCOPE | VENUS - NATIVE TOKEN GATEWAY

10 files audited ● 1 file with Acknowledged findings ● 5 files with Resolved findings ● 4 files without findings

ID	Repo	File	SHA256 Checksum
● NTG	VenusProtocol/isolated-pools	 contracts/Gateway/NativeToken Gateway.sol	a121066a65932b3159ef6eca606917a6e ab2797c728979fdee35617c5ffd8759
● CVP	VenusProtocol/isolated-pools	 contracts/Comptroller.sol	88f346425bd06b12541d0e924c3e92855 7250c07580e0993b13c1dd673c28ad4
● INT	VenusProtocol/isolated-pools	 contracts/Gateway/INativeToken Gateway.sol	72a948702fe425ccb0c77f5528943f9d76 a9e53ad09f067f9a2e824a25ec298
● VTV	VenusProtocol/isolated-pools	 contracts/VToken.sol	7187af56483ac99af75cfd48e978e2ef957 badc084544a519f55c38b9d0c499f
● VBV	VenusProtocol/venus-protocol	 contracts/Tokens/VTokens/VBep 20.sol	d3add14f0773e15df3932888ed771cfb20 dfe18d0c39ea3e9bf21b797118b719
● VTT	VenusProtocol/venus-protocol	 contracts/Tokens/VTokens/VTok en.sol	5e0a06e7ab869ee0b2da14798be2e6682 10c3d2e8b54d073950855cbf48c4cfa
● CSV	VenusProtocol/isolated-pools	 contracts/ComptrollerStorage.sol	a39e9f4631337b05c2c21fef41b0fca9131f 72e2236755e45b7d969baef0e9e3
● IVI	VenusProtocol/isolated-pools	 contracts/Gateway/Interfaces/IV token.sol	a875d842a11fe8d328c58b0b795dac3b44 f8c67f0a76413eec8446134b4abe23
● IWN	VenusProtocol/isolated-pools	 contracts/Gateway/Interfaces/I WrappedNative.sol	3e0f42178c4a04dc537144fdd6efbecb8ae 23d5f2c70135ad3c2fb2bfb8692b1
● VTI	VenusProtocol/isolated-pools	 contracts/VTokenInterfaces.sol	4dde7e54e60abaabcebcc89fdac28bbea8 5b89f4409f1bcdae85fc75e04aae39

APPROACH & METHODS | VENUS - NATIVE TOKEN GATEWAY

This report has been prepared for Venus to discover issues and vulnerabilities in the source code of the Venus - Native Token Gateway 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 - NATIVE TOKEN GATEWAY

This audit concerns the changes made in files outlined in:

- *Isolated Pools*: [PR-361](#)
- *Venus Protocol*: [PR-442](#)

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>.

Overview

The purpose of these PRs were to facilitate the use of native tokens in the wrapped native token markets. For the Isolated-Pools, this was facilitated by adding a new mapping `approvedDelegates` and function `updateDelegate()`, where users can give delegates approval to borrow or redeem on their behalf. For the Core-Pool, this was facilitated by giving the `approvedDelegates` mapping, which already existed in the codebase and gave the ability to borrow on behalf of a user, the additional privilege to redeem on behalf of the user as well.

In addition, a new smart contract `NativeTokenGateway` was added which users can interact with so that they can use native tokens when interacting with the wrapped native token market. The contract allows supplying or repaying using native tokens. It does this by taking the native tokens from the user, wrapping the native tokens, and then supplies or repays the borrow in the wrapped native token market on behalf of the user. The contract also allows redeeming and borrowing for native tokens. It does this by redeeming or borrowing in the wrapped native token market on behalf of the user, unwraps the wrapped native token, and then sends the native tokens to the user.

DEPENDENCIES | VENUS - NATIVE TOKEN GATEWAY

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:

- Wrapped Native Token Contracts

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 - NATIVE TOKEN GATEWAY

8
Total Findings0
Critical1
Major2
Medium0
Minor5
Informational

This report has been prepared to discover issues and vulnerabilities for Venus - Native Token Gateway. Through this audit, we have uncovered 8 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
NTG-04	Centralization Related Risks	Centralization	Major	● Acknowledged
NTG-01	Lack Of Input Validation	Logical Issue	Medium	● Resolved
VBV-01	Extra Approval Will Be Given For Those That Have Already Approved Delegates	Logical Issue	Medium	● Resolved
NTG-05	<code>approve</code> Return Value Not Checked	Coding Style	Informational	● Resolved
NTG-06	Inconsistent Handling Of Wrapped Native Functionality	Logical Issue	Informational	● Resolved
NTG-07	Unnecessary <code>payable</code> Casting	Logical Issue	Informational	● Resolved
NTV-01	Removal Of <code>fallback()</code> Assumes <code>wNativeToken.withdraw()</code> Will Have Empty <code>msg.data</code> When Sending Native Token	Logical Issue	Informational	● Resolved
VPB-01	Typos And Inconsistencies	Inconsistency	Informational	● Resolved

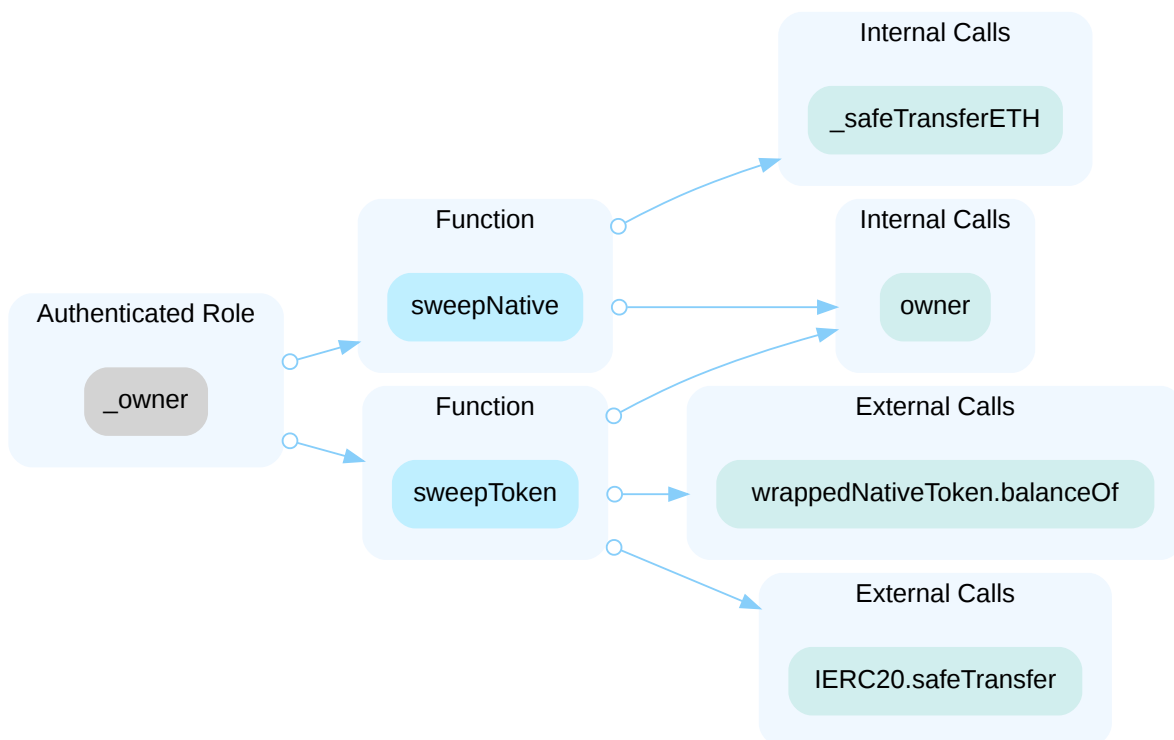
NTG-04 | CENTRALIZATION RELATED RISKS

Category	Severity	Location	Status
Centralization	● Major	contracts/Gateway/NativeTokenGateway.sol (PR361-Base): 146, 160	● Acknowledged

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 `NativeTokenGateway` the role `_owner` has authority over the functions shown in the diagram below. Any compromise to the `_owner` account may allow the hacker to take advantage of this authority and transfer any wrappedNativeToken or native token held by the contract to themselves.



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 ($\frac{2}{3}$, $\frac{3}{5}$) 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.

Alleviation

[Venus, 02/19/2024] : The owner of the NativeTokenGateway contract would be a Normal timelock contract [1], so the mentioned functions will be executable only via Governance.

[1] On BNB chain, this contract is <https://bscscan.com/address/0x939bD8d64c0A9583A7Dcea9933f7b21697ab6396>

[Certik, 02/20/2024] : The client has provided all steps towards mitigation on the BSC chain. In order to mitigate the finding completely, please provide the relevant information corresponding the new networks when they are available.

NTG-01 | LACK OF INPUT VALIDATION

Category	Severity	Location	Status
Logical Issue	● Medium	contracts/Gateway/NativeTokenGateway.sol (PR361-Base): 51, 73, 99, 117	● Resolved

Description

The following functions do not ensure that the input `vToken` is the Venus Wrapped Native Token:

- `wrapAndSupply()`
- `redeemUnderlyingAndUnwrap()`
- `borrowAndUnwrap()`
- `wrapAndRepay()`

This can lead to any tokens that are left in the contract to be stolen or replaced by tokens of lower value by the attacker. Considering the contract is not designed to hold tokens we give this a medium severity.

Scenario

Assume that the contract has a balance of 1000 wrapped native token. An attacker can then do the following:

- Find a token that has a low value compared to the native token that has a market.
- Call `borrowAndUnwrap(vTokenCheap, 1000)` to borrow the `cheapToken`.
- This will then borrow the input `1000 cheapToken` on behalf of the attacker (this will be left in the contract).
- It will then unwrap the contract's 1000 wrapped native token and then transfer 1000 native token to the attacker.

Thus the attacker receives 1000 native token, while the contract gets 1000 cheap token. The attacker can then convert some of the received native token to 1000 cheap token to repay the borrow and profits the rest.

Alternatively, an attacker could input a malicious `vToken` contract that they deployed allowing them to steal the tokens.

Recommendation

We recommend either verifying the input address is the Venus Wrapped Native Token or alternatively making an immutable variable for the Venus Wrapped Native Token address and use this variable as opposed to an input.

Alleviation

[Certik, 02/20/2024]: The client made changes resolving this finding in the commits

- 3c33508cad1667b8bf3c6b07b17fd0d164576420;
- 85271d20aff3e6b9d37ef07faee22ef099a5b8e6.

VBV-01 | EXTRA APPROVAL WILL BE GIVEN FOR THOSE THAT HAVE ALREADY APPROVED DELEGATES

Category	Severity	Location	Status
Logical Issue	● Medium	contracts/Tokens/VTokens/VBep20.sol (PR442-Base): 67, 98	● Resolved

Description

Users that have already approved a delegate in the Core Pool have done so under the assumption that they will only be able to borrow on their behalf. When upgrading to this implementation, those delegates will then have the ability to redeem on their behalf.

Recommendation

We recommend either creating a separate approval for each or providing clear warnings to users that the approval will be extended to include the ability to redeem on their behalf. If the second approach is used, there should be ample time given for users to be made aware of this so that they can revoke the delegate rights if they deem the additional privilege may be dangerous.

Alleviation

[Venus, 02/19/2024] : There are only 4 approved delegates:

borrower: 0x489A8756C18C0b8B24EC2a2b9FF3D4d447F79BEc

delegate: 0x2B16DB59c6f20672C0DB46b80361E9Ca1CD8a43a

TX 1: 0x31f6141db834bb2a286f04b4d3ba002a96a99733cf07eadb043f09f52f489b4b

borrower: 0x8ee5f930571B6e3dA156f678206323213f2A90dc

delegate: 0x85896dAe80a473b5AA60681DB022aebDe766F363

TX 2: 0xc244011c25550080b959593fa87f99fbb1782e98616f5e7c86694ee20a09d22

borrower: 0xB86cb59817E3703589f0FF0dBC5066BffdA0aCDc

delegate: 0xF7eEded9775784A59375a9AB76b034DD63b75595

TX 3: 0x8331870ab6149a7adad2cf4ee9e1b5797d46ba643703d9179493292b0790260e

borrower: 0x489A8756C18C0b8B24EC2a2b9FF3D4d447F79BEc

delegate: 0x89621C48EeC04A85AfadFD37d32077e65aFe2226

TX 4: 0x027c97e0df487cb4cc53f3a70e7ba5aaacfb7ccdf15c652baf80011cfcccf74

The TX 1 and TX 4 were executed in the VIP-99 and VIP-215, respectively. And they shouldn't be a problem due to the special treatment for the affected address (0x489A8756C18C0b8B24EC2a2b9FF3D4d447F79BEc is the BNB Bridge Exploiter account). TX 2 and TX 3 were executed by Venus users. Their balances are small. So, the risk should be low, but just in case we'll announce this change in the VIP where this upgrade will be completed. And we'll announce it in the main Telegram group. Moreover, Natspec comment has been updated to specify clearly:

<https://github.com/VenusProtocol/isolated-pools/commit/18f16c307ef9dd8c3365f9902c2763c388713b14>

NTG-05 | approve RETURN VALUE NOT CHECKED

Category	Severity	Location	Status
Coding Style	● Informational	contracts/Gateway/NativeTokenGateway.sol (PR361-Base): 59, 63, 124, 130	● Resolved

Description

Not all `IERC20` implementations `revert` when there's a failure in `approve`. The function signature has a `boolean` return value and they indicate errors that way instead. By not checking the return value, operations that should have marked as failed, may potentially go through without actually approving anything.

However, `WETH` and `WBNB` would revert when there is a failure in `approve()`.

Recommendation

We recommend considering all possible `wrappedNativeToken` to determine if they will always revert as opposed to returning `false`. If so, then the return value does not need to be checked, however, anytime a new `wrappedNativeToken` is used it should be verified to revert as opposed to returning `false`.

Alternatively, the return value can be checked to be `true`.

Alleviation

[Certik, 02/20/2024]: The client made changes resolving this finding in commit [bfe2c2f0bf5e95bbfe2648f193e202289c26f4f1](#).

Currently the use of `safeApprove()` will not cause any issues as the approval is always set back to zero after the functionality requiring the approval is completed. However, if the contract is changed in the future, then this must be ensured to be preserved.

NTG-06 | INCONSISTENT HANDLING OF WRAPPED NATIVE FUNCTIONALITY

Category	Severity	Location	Status
Logical Issue	● Informational	contracts/Gateway/NativeTokenGateway.sol (PR361-Base): 58, 81~83, 105~106, 123~124, 135~136	● Resolved

Description

In some functions the contract assumes that `wrappedNativeToken.withdraw()` will always give the same amount of `nativeToken` as the input value. Similarly functions assume that `wrappedNativeToken.deposit()` will always give the same amount of `wrappedNativeToken` as the `msg.value`. However, other functions check the before and after balances and do not make this assumption.

Recommendation

We recommend verifying all `wrappedNativeToken` contracts that will be utilized by the protocol are non-upgradeable and give the same amount. If this is the case, then the checking of the before and after amounts can be removed. Alternatively, the before and after amounts for all of these function calls can be checked. If the first option is chosen, then this assumption should be checked for any new `wrappedNativeToken` contracts that this contract is deployed with in the future.

Alleviation

[Certik, 02/20/2024]: The client made changes resolving this finding in commits

- [119cd12084bef3730b877b3a424bc05716e4cd20](#);
- [2c786a004edb6070e7a06587715a55a3af5c895d](#).

NTG-07 | UNNECESSARY payable CASTING

Category	Severity	Location	Status
Logical Issue	● Informational	contracts/Gateway/NativeTokenGateway.sol (PR361-Base): 146	● Resolved

Description

The function `sweepNative()` is designed to be called by the owner in order to transfer any native token balance of the contract to the owner. As such, it does not need to receive native tokens.

Recommendation

We recommend removing the unnecessary payable casting.

Alleviation

[Certik, 02/20/2024]: The client made changes resolving this finding in commit [c05128906cfb983081e87c4a31f410fa1a9a3a18](#).

NTV-01 REMOVAL OF `fallback()` ASSUMES `wNativeToken.withdraw()` WILL HAVE EMPTY `msg.data` WHEN SENDING NATIVE TOKEN

Category	Severity	Location	Status
Logical Issue	● Informational	Gateway/NativeTokenGateway.sol (PR361-Update1): 41~44	● Resolved

Description

The `fallback()` function was removed, which could cause potential issues if `wNativeToken.withdraw()` sends native tokens with non-empty `msg.data`. While current implementations send native tokens with empty `msg.data`, this must be checked anytime a new wrapped native token is to be used.

Recommendation

We recommend either including the `fallback()` function and using the `sweepNative()` function to retrieve any native tokens accidentally sent to the contract or to check that any new supported wrapped native tokens send native tokens with empty `msg.data`.

Alleviation

[Certik, 02/23/2024]: The client made changes resolving this finding in commit [eed3a61c0700ae960e63453b68af947248aabc0d](#).

VPB-01 | TYPOS AND INCONSISTENCIES

Category	Severity	Location	Status
Inconsistency	● Informational	contracts/Comptroller.sol (PR361-Base): 207; contracts/Gateway/INativeTokenGateway.sol (PR361-Base): 33, 58, 65, 72, 79, 85, 90; contracts/Gateway/NativeTokenGateway.sol (PR361-Base): 20, 26, 44, 68, 144, 158, 175; contracts/VToken.sol (PR361-Base): 919; contracts/Comptroller/ComptrollerStorage.sol (PR442-Base): 238~240; contracts/Comptroller/Diamond/facets/MarketFacet.sol (PR442-Base): 201~208, 209, 213; contracts/Tokens/VTokens/VToken.sol (PR442-Base): 845, 867	● Resolved

Description

Core Pool ComptrollerStorage

The comments for `approvedDelegates` do not reflect the added functionality allowing the delegate to redeem.

Core Pool MarketFacet

The comments and inputs for `updateDelegate()` do not reflect the added functionality allowing the delegate to redeem.

Core Pool VToken

The notice for `redeemInternal()` does not reflect the added ability to specify the redeemer and receiver. The notice for `redeemUnderlyingInternal()` does not reflect the added ability to specify the redeemer and receiver.

IsolatedPools VToken

The comments above `_redeemFresh()` do not reflect that users or their delegates can redeem vTokens in exchange for the underlying asset.

Isolated Pools Comptroller

The comments above `updateDelegate()` do not reflect the added functionality allowing the delegate to redeem.

NativeTokenGateway

- The comments above `wrappedNativeToken` use "ether" instead of "native".
- The comments above the `constructor()` use "ether" instead of "native".
- The comments above `wrapAndSupply()` use "vWETH" instead of "vWNative".
- The comments above `redeemUnderlyingAndUnwrap()` use "vWETH" and "ETH" instead of "vWNative" or "native".

- The comments above `sweepNative()` and `sweepToken()` use "Controller" instead of "Controlled".
- The function name `_safeTransferETH()` does not reflect that it is transferring native tokens.

INativeTokenGateway

- The comment for the event `sweepToken` uses "WETH" instead of "WNative".
- The comments for `wrapAndSupply()`, `redeemUnderlyingAndUnwrap()`, `borrowAndUnwrap()`, `wrapAndRepay()`, `sweepToken()`, and `sweepNative()` reference "ETH", "WETH", and "vWETH".

Recommendation

We recommend correcting the typos and inconsistencies above.

Alleviation

[Certik, 02/23/2024]: The client made changes resolving this finding in commits

- [9bad33fbda0631a7b85e14d1eae0aae8e545842d](#);
- [becfe891329b8c93f46e968051721848d6d05253](#);
- [dfaef87d68aa22b5b75883debadf3ef8cb05cd58](#);
- [e81ab4feaa5a2e62c27a5532251931b3ce749741](#)
- [dbd4edcd43bee1a80b57fe034259653eef158e92](#)
- [6580956148fd16685bb0d456cbef0d7a97e69025](#)

APPENDIX | VENUS - NATIVE TOKEN GATEWAY

Finding Categories

Categories	Description
Coding Style	Coding Style findings may not affect code behavior, but indicate areas where coding practices can be improved to make the code more understandable and maintainable.
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.

