CERTIK

Venus - PendleOracle Upgrade

Security Assessment

CertiK Assessed on Dec 26th, 2024

CertiK Assessed on Dec 26th, 2024

Venus - PendleOracle Upgrade

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

Executive Summary

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

LANGUAGE	TIMELINE	KEY COMPONENTS
Solidity	Delivered on 12/26/2024	N/A

CODEBASE

https://github.com/VenusProtocol/oracle

View All in Codebase Page

COMMITS

Base: 97d37973628a56f8bbd1a8c6d0b3301602fe4aae

Update: d53f26567c18f0f10f8ad743f9cfbf2a5388f2f1

View All in Codebase Page

Vulnerability Summary

3	2	0	0	1	0
Total Findings	Resolved	Mitigated	Partially Resolved	Acknowledged	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.
🟨	1	Medium	1 Resolved	Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.
🟨	1	Minor	1 Acknowledged	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 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 - PENDLEORACLE UPGRADE

CODEBASE | VENUS - PENDLEORACLE UPGRADE

Repository

https://github.com/VenusProtocol/oracle

Commit

Base: 97d37973628a56f8bbd1a8c6d0b3301602fe4aae

Update: d53f26567c18f0f10f8ad743f9cfbf2a5388f2f1

AUDIT SCOPE | VENUS - PENDLEORACLE UPGRADE

2 files audited ● 2 files without findings

ID	Repo	File	SHA256 Checksum
● POV	VenusProtocol/oracle	PendleOracle.sol	6a61f432fab284d10230f725581f14d42450b1c29c9af9daf898505e357a0f78
● IPP	VenusProtocol/oracle	IPendlePtOracle.sol	d1f470d0d38eb100dd75e12d285d2e6bcb3df215595ed556e5524d899487d6af

APPROACH & METHODS | VENUS - PENDLEORACLE UPGRADE

This report has been prepared for Venus to discover issues and vulnerabilities in the source code of the Venus - PendleOracle Upgrade 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 - PENDLEORACLE UPGRADE

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

- https://github.com/VenusProtocol/oracle/pull/240

Note that any centralization risks present in the existing codebase before this PR 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, this PR is designed to upgrade the current implementation of the `PendleOracle` contract to add support for for Pendle's `getPtToSyRate()` . This allows the ability to add yield tokens as a base, as an alternative to using the underlying asset directly.

DEPENDENCIES | VENUS - PENDLEORACLE UPGRADE

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:

- Third Party Token Contracts
- Third Party Oracles

The scope of the audit treats third party entities as black boxes and assumes their functional correctness. However, in the real world, third parties can be compromised and this may lead to lost or stolen assets. Moreover, updates to the state of a project contract that are dependent on the read of the state of external third party contracts may make the project vulnerable to read-only reentrancy. In addition, upgrades of third parties can possibly create severe impacts, such as returning invalid prices, returning invalid exchange rates, 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 - PENDLEORACLE UPGRADE

3	0	0	1	1	1
Total Findings	Critical	Major	Medium	Minor	Informational

This report has been prepared to discover issues and vulnerabilities for Venus - PendleOracle Upgrade. Through this audit, we have uncovered 3 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
POV-01	Pendle Oracle Does Not Always Return Rate Scaled By The Underlying Decimals	Logical Issue	Medium	● Resolved
POV-02	No Check That Underlying Token Is Consistent With Rate Kind	Logical Issue	Minor	● Acknowledged
POV-03	Inconsistent Comment	Inconsistency	Informational	● Resolved

POV-01 PENDLE ORACLE DOES NOT ALWAYS RETURN RATE SCALED BY THE UNDERLYING DECIMALS

Category	Severity	Location	Status
Logical Issue	● Medium	PendleOracle.sol (PendleOracle Base): 80~85	● Resolved

Description

The function `_getUnderlyingAmount()` is designed to get the `underlyingToken` amount for 1 `ptToken` scaled by the `underlyingToken` decimals. However, this function simply returns the value obtained from the `PT_ORACLE` , which does not always have this scaling and can result in an incorrect price being returned.

For example lets assume that PT pumpBTC 27MAR2025 is to be supported 0x997Ec6Bf18a30Ef01ed8D9c90718C7726a213527. If one uses the `PendlePtLpOracle` at address 0x66a1096C6366b2529274dF4f5D8247827fe4CEA8 (currently used by Venus) and fetches the rate via the pumpBTC market 0x8098b48a1c4e4080b30a43a7ebc0c87b52f17222, it will return a value with 18 decimals of precision, however WBTC only has 8 decimals. This would result in the wrong price being returned.

In our testing when calling `PT_ORACLE.getPtToAssetRate(0x8098b48a1c4e4080b30a43a7ebc0c87b52f17222, 900)` we got a value of `988245041751264715` , which is scaled by 1e18 as opposed to 1e8.

Scenario

Assume that the following inputs are used to deploy a new instance of the Pendle oracle.

- market = 0x8098b48a1c4e4080b30a43a7ebc0c87b52f17222 (pumpBTC market);
- ptOracle = 0x66a1096C6366b2529274dF4f5D8247827fe4CEA8 (PendlePtLpOracle);
- rateKind = PT_TO_ASSET;
- ptToken = 0x997Ec6Bf18a30Ef01ed8D9c90718C7726a213527 (PT pumpBTC 27MAR2025);
- underlyingToken = 0x2260FAC5E5542a773Aa44fBCfeDf7C193bc2C599 (WBTC);

Then if `getPrice(0x997Ec6Bf18a30Ef01ed8D9c90718C7726a213527)` from the `CorrelatedTokenOracle` is called (link) it will return a price with 38 decimals of precision when it should return a price with 36 - correlated token decimals = 36 - 8 = 28 decimals of precision.

This is because in the calculation of the price

```
underlyingAmount = _getUnderlyingAmount()
```

will have 18 decimals of precision and

```
uint256 underlyingUSDPrice = RESILIENT_ORACLE.getPrice(UNDERLYING_TOKEN)
```

will have `36-8 = 28` decimals of precision (because the RESILIENT_ORACLE returns a price with 36 - UNDERLYING_TOKEN decimals of precision and the UNDERLYING_TOKEN is WBTC which has 8 decimals). Thus the return value

```
IERC20Metadata token = IERC20Metadata(CORRELATED_TOKEN);
uint256 decimals = token.decimals();

return (underlyingAmount * underlyingUSDPrice) / (10 ** decimals);
```

will have 18 + 28 - 8 = 38 decimals of precision (because PT pumpBTC 27MAR2025 is the CORRELATED_TOKEN and has 8 decimal).

This demonstrates how `getPrice()` will return an incorrect price if such a market is supported.

Recommendation

We recommend ensuring that `_getUnderlyingAmount()` returns an amount scaled by the underlying token decimals for all Pendle oracles/markets that will be supported.

POV-02 | NO CHECK THAT UNDERLYING TOKEN IS CONSISTENT WITH RATE KIND

Category	Severity	Location	Status
Logical Issue	● Minor	PendleOracle.sol (PendleOracle Base): 64	● Acknowledged

Description

The function `_getUnderlyingAmount()` returns the amount of `underlyingToken` for 1 pendle token. If `RATE_KIND = PT_TO_SY`, then it returns the amount of SY for 1 pendle token, so that in this case the `underlyingToken` should be the SY token. Alternatively, if `RATE_KIND = PT_TO_ASSET`, then it returns the amount of underlying asset for 1 pendle token, so that in this case the `underlyingToken` should be underlying asset.

However, there are no checks in the `constructor()` ensuring that the correct `underlyingToken` is chosen for the input `rateKind`. If these inputs are not consistent, then the oracle will return an incorrect price.

Recommendation

We recommend adding checks in the `constructor()` to ensure that the input `underlyingToken` is consistent with the input `rateKind`.

POV-03 | INCONSISTENT COMMENT

Category	Severity	Location	Status
Inconsistency	● Informational	PendleOracle.sol (PendleOracle Base): 77, 78	● Resolved

Description

The comment above `_getUnderlyingAmount()` was updated to state that it fetches the amount of underlying or SY token for 1 pendle token. However, this may be misunderstood, because in the case that `RATE_KIND == PT_TO_SY` the `underlyingToken` should be set to the SY token.

Recommendation

We recommend adjusting the comments to avoid any confusion as "underlying" can be understood to be the underlying asset of the PT token or the `underlyingToken` set in the constructor, which are not always the same.

APPENDIX | VENUS - PENDLEORACLE UPGRADE

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.

Checksum Calculation Method

The "Checksum" field in the "Audit Scope" section is calculated as the SHA-256 (Secure Hash Algorithm 2 with digest size of 256 bits) digest of the content of each file hosted in the listed source repository under the specified commit.

The result is hexadecimal encoded and is the same as the output of the Linux "sha256sum" command against the target file.

DISCLAIMER | CERTIK

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you ("Customer" or the "Company") in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without CertiK's prior written consent in each instance.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts CertiK to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. CertiK's position is that each company and individual are responsible for their own due diligence and continuous security. CertiK's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by CertiK is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, CERTIK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, CERTIK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, CERTIK MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE. WITHOUT LIMITATION TO THE FOREGOING, CERTIK PROVIDES NO WARRANTY OR

UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER CERTIK NOR ANY OF CERTIK'S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. CERTIK WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER'S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT CERTIK'S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF CERTIK CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

Elevating Your Entire Web3 Journey

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we're able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.