SMART CONTRACT AUDIT REPORT

for

Venus PSM

Prepared By: Xiaomi Huang

PeckShield

April 26, 2023

Document Properties

Client	Venus
Title	Smart Contract Audit Report
Target	Venus PSM
Version	1.0
Author	Xuxian Jiang
Auditors	Xiaotao Wu, Xuxian Jiang
Reviewed by	Xiaomi Huang
Approved by	Xuxian Jiang
Classification	Public

Version Info

Version	Date	Author(s)	Description
1.0	April 26, 2023	Xuxian Jiang	Final Release
1.0-rc	April 22, 2023	Xuxian Jiang	Release Candidate

Contact

For more information about this document and its contents, please contact PeckShield Inc.

Name	Xiaomi Huang
Phone	+86 183 5897 7782
Email	contact@peckshield.com

Contents

1 Introduction

Given the opportunity to review the design document and related smart contract source code of the PSM feature in Venus, we outline in the report our systematic approach to evaluate potential security issues in the smart contract implementation, expose possible semantic inconsistencies between smart contract code and design document, and provide additional suggestions or recommendations for improvement. Our results show that the given version of smart contracts can be further improved due to the presence of several issues related to either security or performance. This document outlines our audit results.

1.1 About Venus PSM

The Venus protocol is designed to enable a complete algorithmic money market protocol on Binance Smart Chain (BSC). Venus enables users to utilize their cryptocurrencies by supplying collateral to the protocol that may be borrowed by pledging over-collateralized cryptocurrencies. The audited PSM feature is a mechanism designed to ensure the peg of VAI to 1. The contract enables users to swap VAI and another stablecoin (USDT or USDC) at a fixed conversion rate. The PSM can create a more stable and liquid environment for VAI trading, thus helping maintain its peg. The basic information of the audited protocol is as follows:

Table 1.1: Basic Information of The Venus PSM

Item	Description
Name	Venus
Website	https://venus.io/
Type	EVM Smart Contract
Platform	Solidity
Audit Method	Whitebox
Latest Audit Report	April 26, 2023

In the following, we show the Git repository of reviewed files and the commit hash value used in this audit:

- https://github.com/VenusProtocol/venus-protocol/pull/247 (75148f1)

1.2 About PeckShield

PeckShield Inc. [7] is a leading blockchain security company with the goal of elevating the security, privacy, and usability of current blockchain ecosystems by offering top-notch, industry-leading services and products (including the service of smart contract auditing). We are reachable at Telegram (https://t.me/peckshield), Twitter (http://twitter.com/peckshield), or Email (contact@peckshield.com).

Table 1.2: Vulnerability Severity Classification

Impact \ **Likelihood**	*High*	*Medium*	*Low*
High	Critical	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

1.3 Methodology

To standardize the evaluation, we define the following terminology based on OWASP Risk Rating Methodology [6]:

- Likelihood represents how likely a particular vulnerability is to be uncovered and exploited in the wild;
- Impact measures the technical loss and business damage of a successful attack;
- Severity demonstrates the overall criticality of the risk.

Likelihood and impact are categorized into three ratings: *H*, *M* and *L*, i.e., *high*, *medium* and *low* respectively. Severity is determined by likelihood and impact and can be classified into four categories accordingly, i.e., *Critical*, *High*, *Medium*, *Low* shown in Table 1.2.

To evaluate the risk, we go through a list of check items and each would be labeled with a severity category. For one check item, if our tool or analysis does not identify any issue, the contract is considered safe regarding the check item. For any discovered issue, we might further

Table 1.3: The Full List of Check Items

Category	Check Item
Basic Coding Bugs	Constructor Mismatch
	Ownership Takeover
	Redundant Fallback Function
	Overflows & Underflows
	Reentrancy
	Money-Giving Bug
	Blackhole
	Unauthorized Self-Destruct
	Revert DoS
	Unchecked External Call
	Gasless Send
	Send Instead Of Transfer
	Costly Loop
	(Unsafe) Use Of Untrusted Libraries
	(Unsafe) Use Of Predictable Variables
	Transaction Ordering Dependence
	Deprecated Uses
Semantic Consistency Checks	Semantic Consistency Checks
Advanced DeFi Scrutiny	Business Logics Review
	Functionality Checks
	Authentication Management
	Access Control & Authorization
	Oracle Security
	Digital Asset Escrow
	Kill-Switch Mechanism
	Operation Trails & Event Generation
	ERC20 Idiosyncrasies Handling
	Frontend-Contract Integration
	Deployment Consistency
	Holistic Risk Management
Additional Recommendations	Avoiding Use of Variadic Byte Array
	Using Fixed Compiler Version
	Making Visibility Level Explicit
	Making Type Inference Explicit
	Adhering To Function Declaration Strictly
	Following Other Best Practices

deploy contracts on our private testnet and run tests to confirm the findings. If necessary, we would additionally build a PoC to demonstrate the possibility of exploitation. The concrete list of check items is shown in Table 1.3.

In particular, we perform the audit according to the following procedure:

- Basic Coding Bugs: We first statically analyze given smart contracts with our proprietary static code analyzer for known coding bugs, and then manually verify (reject or confirm) all the issues found by our tool.
- Semantic Consistency Checks: We then manually check the logic of implemented smart contracts and compare with the description in the white paper.
- Advanced DeFi Scrutiny: We further review business logics, examine system operations, and place DeFi-related aspects under scrutiny to uncover possible pitfalls and/or bugs.
- Additional Recommendations: We also provide additional suggestions regarding the coding and development of smart contracts from the perspective of proven programming practices.

To better describe each issue we identified, we categorize the findings with Common Weakness Enumeration (CWE-699) [5], which is a community-developed list of software weakness types to better delineate and organize weaknesses around concepts frequently encountered in software development. Though some categories used in CWE-699 may not be relevant in smart contracts, we use the CWE categories in Table 1.4 to classify our findings.

1.4 Disclaimer

Note that this security audit is not designed to replace functional tests required before any software release, and does not give any warranties on finding all possible security issues of the given smart contract(s) or blockchain software, i.e., the evaluation result does not guarantee the nonexistence of any further findings of security issues. As one audit-based assessment cannot be considered comprehensive, we always recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contract(s). Last but not least, this security audit should not be used as investment advice.

Table 1.4: Common Weakness Enumeration (CWE) Classifications Used in This Audit

Category	Summary
Configuration	Weaknesses in this category are typically introduced during the configuration of the software.
Data Processing Issues	Weaknesses in this category are typically found in functionality that processes data.
Numeric Errors	Weaknesses in this category are related to improper calculation or conversion of numbers.
Security Features	Weaknesses in this category are concerned with topics like authentication, access control, confidentiality, cryptography, and privilege management. (Software security is not security software.)
Time and State	Weaknesses in this category are related to the improper management of time and state in an environment that supports simultaneous or near-simultaneous computation by multiple systems, processes, or threads.
Error Conditions, Return Values, Status Codes	Weaknesses in this category include weaknesses that occur if a function does not generate the correct return/status code, or if the application does not handle all possible return/status codes that could be generated by a function.
Resource Management	Weaknesses in this category are related to improper management of system resources.
Behavioral Issues	Weaknesses in this category are related to unexpected behaviors from code that an application uses.
Business Logics	Weaknesses in this category identify some of the underlying problems that commonly allow attackers to manipulate the business logic of an application. Errors in business logic can be devastating to an entire application.
Initialization and Cleanup	Weaknesses in this category occur in behaviors that are used for initialization and breakdown.
Arguments and Parameters	Weaknesses in this category are related to improper use of arguments or parameters within function calls.
Expression Issues	Weaknesses in this category are related to incorrectly written expressions within code.
Coding Practices	Weaknesses in this category are related to coding practices that are deemed unsafe and increase the chances that an exploitable vulnerability will be present in the application. They may not directly introduce a vulnerability, but indicate the product has not been carefully developed or maintained.

2 Findings

2.1 Summary

Here is a summary of our findings after analyzing the Venus's PSM implementation. During the first phase of our audit, we study the smart contract source code and run our in-house static code analyzer through the codebase. The purpose here is to statically identify known coding bugs, and then manually verify (reject or confirm) issues reported by our tool. We further manually review business logics, examine system operations, and place DeFi-related aspects under scrutiny to uncover possible pitfalls and/or bugs.

Severity	# of Findings	
Critical	0	
High	0	
Medium	0	
Low	2	■ ■
Informational	0	
Total	2	

We have so far identified a list of potential issues: some of them involve subtle corner cases that might not be previously thought of, while others refer to unusual interactions among multiple contracts. For each uncovered issue, we have therefore developed test cases for reasoning, reproduction, and/or verification. After further analysis and internal discussion, we determined a few issues of varying severities that need to be brought up and paid more attention to, which are categorized in the above table. More information can be found in the next subsection, and the detailed discussions of each of them are in Section 3.

2.2 Key Findings

Overall, these smart contracts are well-designed and engineered, though the implementation can be improved by resolving the identified issues (shown in Table 2.1), including 2 low-severity vulnerabilities.

Table 2.1: Key Venus PSM Audit Findings

ID	Severity	Title	Category	Status
PVE-001	Low	Inconsistent Fee Validation Logic in PegStability	Business Logic	Resolved
PVE-002	Low	Trust Issue of Admin Keys	Security Features	Resolved

Besides recommending specific countermeasures to mitigate these issues, we also emphasize that it is always important to develop necessary risk-control mechanisms and make contingency plans, which may need to be exercised before the mainnet deployment. The risk-control mechanisms need to kick in at the very moment when the contracts are being deployed in mainnet. Please refer to Section 3 for details.

3 | Detailed Results

3.1 Inconsistent Fee Validation Logic in PegStability

- ID: PVE-001
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: PegStability
- Category: Coding Practices [4]
- CWE subcategory: CWE-1126 [1]

Description

DeFi protocols typically have a number of system-wide parameters that can be dynamically configured on demand. The Venus's PSM module is no exception. Specifically, if we examine the PegStability contract, it has defined a number of protocol-wide risk parameters, such as feeIn/feeOut and vaiMintCap. In the following, we show the corresponding routines that allow for their changes.

```
    function setFeeIn(uint256 feeIn_) external {
        _checkAccessAllowed("setFeeIn(uint256)");
        // feeIn = 10000 = 100%
        require(feeIn_ < BASIS_POINTS_DIVISOR, "Invalid fee.");
        uint256 oldFeeIn = feeIn;
        feeIn = feeIn_;
        emit FeeInChanged(oldFeeIn, feeIn_);
    }

    /**
     * @notice Set the fee percentage for outgoing swaps
     * @dev Reverts if the new fee percentage is invalid (greater than or equal to
         BASIS_POINTS_DIVISOR)
     * @param feeOut_ The new fee percentage for outgoing swaps
     */
    // @custom:event Emits FeeOutChanged event
    function setFeeOut(uint256 feeOut_) external {
        _checkAccessAllowed("setFeeOut(uint256)");
        // feeOut = 10000 = 100%
        require(feeOut_ < BASIS_POINTS_DIVISOR, "Invalid fee.");
        uint256 oldFeeOut = feeOut;
```

```
        feeOut = feeOut_;
        emit FeeOutChanged(oldFeeOut, feeOut_);
    }
```

Listing 3.1: PegStability :: setFeeIn()/setFeeOut()

These parameters define various aspects of the protocol operation and maintenance and need to exercise extra care when configuring or updating them. Our analysis shows the update logic on these parameters can be improved by applying more rigorous sanity checks. Based on the current implementation, we notice the configured `feeIn/FeeOut` can be consistently validated. For example, the following `initialize()` routine does not validate the given `feeIn/FeeOut` to ensure they are always smaller than `BASIS_POINTS_DIVISOR`.

```
    function initialize(
        address accessControlManager_,
        address venusTreasury_,
        address priceOracle_,
        uint256 feeIn_,
        uint256 feeOut_,
        uint256 vaiMintCap_
    ) external initializer {
        ensureNonzeroAddress(accessControlManager_);
        ensureNonzeroAddress(venusTreasury_);
        ensureNonzeroAddress(priceOracle_);
        __AccessControlled_init(accessControlManager_);
        feeIn = feeIn_;
        feeOut = feeOut_;
        vaiMintCap = vaiMintCap_;
        venusTreasury = venusTreasury_;
        priceOracle = priceOracle_;
    }
```

Listing 3.2: PegStability :: initialize ()

Recommendation Consistently validate the protocol parameters to ensure that they always fall in an appropriate range.

Status The issue has been fixed by this commit: `9976024`.

3.2 Trust Issue of Admin Keys

- ID: PVE-002
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: PegStability
- Category: Security Features [3]
- CWE subcategory: CWE-287 [2]

Description

In the PegStability module, there is a privileged accessControlManager_ account that plays a critical role in governing and regulating the system-wide operations (e.g., configure protocol parameters and set up the price oracle). In the following, we use the PegStability contract as an example and show the representative functions potentially affected by the privileges of the account.

```
    function setVaiMintCap(uint256 vaiMintCap_) external {
        _checkAccessAllowed("setVaiMintCap(uint256)");
        uint256 oldVaiMintCap = vaiMintCap;
        vaiMintCap = vaiMintCap_;
        emit VaiMintCapChanged(oldVaiMintCap, vaiMintCap);
    }

    /**
     * @notice Set the address of the Venus Treasury contract
     * @dev Reverts if the new address is zero
     * @param venusTreasury_ The new address of the Venus Treasury contract
     */
    // @custom:event Emits VenusTreasuryChanged event
    function setVenusTreasury(address venusTreasury_) external {
        _checkAccessAllowed("setVenusTreasury(address)");
        ensureNonzeroAddress(venusTreasury_);
        address oldTreasuryAddress = venusTreasury;
        venusTreasury = venusTreasury_;
        emit VenusTreasuryChanged(oldTreasuryAddress, venusTreasury_);
    }

    /**
     * @notice Set the address of the PriceOracle contract
     * @dev Reverts if the new address is zero
     * @param priceOracle_ The new address of the PriceOracle contract
     */
    // @custom:event Emits PriceOracleChanged event
    function setPriceOracle(address priceOracle_) external {
        _checkAccessAllowed("setPriceOracle(address)");
        ensureNonzeroAddress(priceOracle_);
        address oldPriceOracleAddress = priceOracle_;
        priceOracle = priceOracle_;
        emit PriceOracleChanged(oldPriceOracleAddress, priceOracle_);
```

```
    }
```

Listing 3.3: Example Privileged Operations in the `PegStability` Contract

We understand the need of the privileged functions for contract maintenance, but at the same time the extra power to the privileged account may also be a counter-party risk to the protocol users. It is worrisome if the privileged account is a plain EOA account. Note that a multi-sig account could greatly alleviate this concern, though it is still far from perfect. Specifically, a better approach is to eliminate the administration key concern by transferring the role to a community-governed DAO.

Recommendation Promptly transfer the privileged accounts to the intended `DAO`-like governance contract. All changed to privileged operations may need to be mediated with necessary timelocks. Eventually, activate the normal on-chain community-based governance life-cycle and ensure the intended trustless nature and high-quality distributed governance.

Status This issue has been confirmed and the team has explicitly stated the use of a timelock for the above admin account.

4 Conclusion

In this audit, we have analyzed the Venus's PSM design and implementation. The audited PSM feature is a mechanism designed to ensure the peg of VAI to 1. The contract enables users to swap VAI and another stablecoin (USDT or USDC) at a fixed conversion rate. The PSM can create a more stable and liquid environment for VAI trading, thus helping maintain its peg. The current code base is well structured and neatly organized. Those identified issues are promptly confirmed and addressed.

Meanwhile, we need to emphasize that Solidity-based smart contracts as a whole are still in an early, but exciting stage of development. To improve this report, we greatly appreciate any constructive feedbacks or suggestions, on our methodology, audit findings, or potential gaps in scope/coverage.

References

[1] MITRE. CWE-1126: Declaration of Variable with Unnecessarily Wide Scope. https://cwe.mitre.org/data/definitions/1126.html.

[2] MITRE. CWE-287: Improper Authentication. https://cwe.mitre.org/data/definitions/287.html.

[3] MITRE. CWE CATEGORY: 7PK - Security Features. https://cwe.mitre.org/data/definitions/254.html.

[4] MITRE. CWE CATEGORY: Bad Coding Practices. https://cwe.mitre.org/data/definitions/1006.html.

[5] MITRE. CWE VIEW: Development Concepts. https://cwe.mitre.org/data/definitions/699.html.

[6] OWASP. Risk Rating Methodology. https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

[7] PeckShield. PeckShield Inc. https://www.peckshield.com.