SMART CONTRACT AUDIT REPORT

for

NFTProtocolDEX V3

Prepared By: Xiaomi Huang

PeckShield

August 16, 2022

Document Properties

Client	NFT Protocol
Title	Smart Contract Audit Report
Target	NFTProtocolDEX V3
Version	1.0
Author	Shulin Bie
Auditors	Shulin Bie, Xuxian Jiang
Reviewed by	Xiaomi Huang
Approved by	Xuxian Jiang
Classification	Public

Version Info

Version	Date	Author(s)	Description
1.0	August 16, 2022	Shulin Bie	Final Release
1.0-rc	August 12, 2022	Shulin Bie	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 NFTProtocolDEX V3 protocol, 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 NFTProtocolDEX V3

NFTProtocolDEX V3 is a decentralized exchange protocol that is designed to facilitate the safe, secure and trustless exchange of NFTs with other assets. It supports the ERC721, ERC1155, and ERC20 token standards as well as native assets (e.g., ETH/MATIC). It allows users to create and fill 1:1 or multi-asset swap order involving any combination and quantity of supported asset types. The basic information of the audited protocol is as follows:

Table 1.1: Basic Information of NFTProtocolDEX V3

Item	Description
Target	NFTProtocolDEX V3
Type	EVM Smart Contract
Language	Solidity
Audit Method	Whitebox
Latest Audit Report	August 16, 2022

In the following, we show the Git repository of reviewed files and the commit hash value used in this audit. Please note this audit only covers the v3.0 sub-directory.

- https://github.com/nftprotocol/nft-dex-audit.git (12e2d4e)

And this is the commit ID after all fixes for the issues found in the audit have been checked in:

- https://github.com/nftprotocol/nft-dex-audit.git (e4a0960)

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

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

contract is considered safe regarding the check item. For any discovered issue, we might further 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 `NFTProtocolDEX V3` 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 logic, 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	1	■
Low	2	■ ■
Informational	0	
Total	3	

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 1 medium-severity vulnerability and 2 low-severity vulnerabilities.

Table 2.1: Key NFTProtocolDEX V3 Audit Findings

ID	Severity	Title	Category	Status
PVE-001	Medium	Possible Front-running Attack for takeSwap()	Time And State	Fixed
PVE-002	Low	Flashloan-Assisted Fee Avoidance in takeSwap()	Time And State	Confirmed
PVE-003	Low	Trust Issue of Admin Keys	Security Features	Confirmed

Beside the identified issues, we emphasize that for any user-facing applications and services, 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 should kick in at the very moment when the contracts are being deployed on mainnet. Please refer to Section 3 for details.

3 | Detailed Results

3.1 Possible Front-running Attack for takeSwap()

- ID: PVE-001
- Severity: Medium
- Likelihood: Medium
- Impact: Medium
- Target: NFTProtocolDEX
- Category: Time and State [4]
- CWE subcategory: CWE-682 [2]

Description

The NFTProtocolDEX V3 protocol allows users to participate as maker or taker. The maker can create and fill a 1:1 or multi-assets swap order specifying the assets that he intends to sell and buy via the makeSwap() routine, while the taker can buy the assets that the maker intends to sell in the swap order via the takeSwap() routine. Additionally, the maker has capability to amend the sell or buy ETH amount in his swap order via the amendSwapEther() routine.

Our analysis shows the takeSwap() routine is exposed to a potential front-running attack. The malicious maker can launch a front-running amendSwapEther() operation. With that, he may get the taker's assets with 0 ETH.

```
    function takeSwap(uint256 swapID_) external payable override unlocked notOwner nonReentrant {
        address sender = _msgSender();
        (Swap storage swp, uint256 pay, uint256 updated, uint256 fee) = _takerSwapAndValues(sender, swapID_, msg.value);
        require(msg.value >= pay, "Insufficient Ether value (price + fee)");

        // Close out swap.
        swp.status = CLOSED_SWAP;
        swp.taker = sender;

        // Update balance.
        _updateBalance(updated, swapID_);

        // Transfer assets from DEX to taker.
```

```
        _transferAssetsOut(swp.components[MAKER_SIDE], swp.maker, swp.custodial);

        // Transfer assets from taker to maker.
        for (uint256 i = 0; i < swp.components[TAKER_SIDE].length; i++) {
            _transferAsset(swp.components[TAKER_SIDE][i], sender, swp.maker);
        }

        // Credit fee to owner.
        address owner_ = owner();
        _balances[owner_] += fee;
        tvl += msg.value;
        tvl -= fee;

        // Issue events.
        emit SwapTaken(swapID_, sender, fee);
        emit Deposited(owner(), fee);
    }

    function amendSwapEther(uint256 swapID_, uint8 side_, uint256 value_) external
        payable override unlocked notOwner nonReentrant validSide(side_) validSwap(
        swapID_) {
        Swap storage swp = _swaps[swapID_];
        require(swp.status == OPEN_SWAP, "Swap not open");
        address sender = _msgSender();
        require(sender == swp.maker, "Not swap maker");
        require(_notExpired(swp.expiration), "Swap expired");
        Component[] storage comps = swp.components[side_];

        // Set ether asset.
        (uint256 previous, uint256 index) = _setEtherAsset(comps, value_);
        require(value_ != previous, "Ether value unchanged");
        require(value_ > 0  comps.length > 1, "Swap side becomes empty");

        // Update balance.
        uint256 balance_ = _balances[sender];
        if (side_ == TAKER_SIDE && msg.value > 0) {
            _updateBalance(balance_ + msg.value, swapID_);
        } else if (side_ == MAKER_SIDE) {
            if (value_ > previous) {
                require(balance_ + msg.value >= value_ - previous, "Insufficient Ether
                    value");
            }
            _updateBalance(balance_ + msg.value + previous - value_, swapID_);
        }

        // Update tvl.
        tvl += msg.value;

        // Issue event.
        emit SwapEtherAmended(swapID_, side_, index, previous, value_);
    }
```

Listing 3.1: NFTProtocolDEX::takeSwap()/amendSwapEther()

Recommendation Add necessary protection in above-mentioned `takeSwap()` routine to prevent potential `front-running` attack.

Status The issue has been addressed in this commit: `e4a0960`.

3.2 Flashloan-Assisted Fee Avoidance in takeSwap()

- ID: PVE-002
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: `NFTProtocolDEX`
- Category: Time and State [4]
- CWE subcategory: CWE-682 [2]

Description

As mentioned in Section 3.1, the `takeSwap()` routine is used by the `taker` to buy the assets that the maker intends to sell in the swap order. Meanwhile, the privileged `owner` will charge a certain amount of `ETH` as trade fee from the `taker`. The calculation of trade fee depends on the balance of the `taker`'s `ERC20 NFT Protocol` token. If the balance is greater than or equal to `highFee`, the trade fee will be 0. Our analysis shows this can be exploited by the `taker` to avoid trade fee.

To elaborate, we show below the related code snippet of the `takerFeeWith()` routine. To avoid any fee charge, a `taker` may flash borrow enough `ERC20 NFT Protocol` token before calling `takeSwap()` and repay the borrowed token after calling `takeSwap()`.

```
    function takerFeeWith(address sender_) public view override unlocked returns (
        uint256) {
        uint256 balance_ = IERC20(token).balanceOf(sender_);
        if (balance_ >= highFee) {
            return 0;
        }
        if (balance_ < lowFee) {
            return flatFee;
        }
        // Take 10% off as soon as feeBypassLow is reached.
        uint256 startFee = (flatFee * 9) / 10;
        return startFee - (startFee * (balance_ - lowFee)) / (highFee - lowFee);
    }
```

Listing 3.2: `NFTProtocolDEX::takerFeeWith()`

Recommendation Optimize the fee charge mechanism used in the `takerFeeWith()` routine.

Status The issue has been confirmed by the team.

3.3 Trust Issue of Admin Keys

- ID: PVE-003
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: NFTProtocolDEX
- Category: Security Features [3]
- CWE subcategory: CWE-287 [1]

Description

In the NFTProtocolDEX V3 protocol, there is a privileged owner account that plays a critical role in governing and regulating the protocol-wide operations (e.g., configuring various system parameters). In the following, we show a representative function potentially affected by the privilege of the owner account.

```
    function setFees(
        uint256 flatFee_,
        uint256 lowFee_,
        uint256 highFee_
    ) external override supported onlyOwner {
        require(lowFee_ <= highFee_, "lowFee must be <= highFee");
        flatFee = flatFee_;
        lowFee = lowFee_;
        highFee = highFee_;
        emit FeesChanged(flatFee, lowFee, highFee);
    }
```

Listing 3.3: NFTProtocolDEX::setFees()

We emphasize that the privilege assignment is indeed necessary and consistent with the protocol design. However, it is worrisome if the privileged account is a plain EOA account. A multi-sig account could greatly alleviate this concern, though it is still far from perfect. Note that a compromised privileged account would allow the attacker to modify a number of sensitive system parameters, which directly undermines the assumption of the protocol design.

Recommendation Suggest a multi-sig account plays the privileged owner account to mitigate this issue. Additionally, all changes to privileged operations may need to be mediated with necessary timelocks.

Status The issue has been confirmed by the team.

4 Conclusion

In this audit, we have analyzed the `NFTProtocolDEX V3` design and implementation. The `NFTProtocolDEX V3` is a decentralized exchange protocol designed to facilitate the safe, secure and trustless exchange of NFTs with other assets. It allows users to create and fill `1:1` or multi-asset swap order involving any combination and quantity of supported asset types (including `ERC721`, `ERC1155`, `ERC20`, and `ETH/MATIC`). The current code base is well structured and neatly organized. Those identified issues are promptly confirmed and addressed.

Meanwhile, we need to emphasize that 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-287: Improper Authentication. https://cwe.mitre.org/data/definitions/287.html.

[2] MITRE. CWE-682: Incorrect Calculation. https://cwe.mitre.org/data/definitions/682.html.

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

[4] MITRE. CWE CATEGORY: Error Conditions, Return Values, Status Codes. https://cwe.mitre.org/data/definitions/389.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.