SMART CONTRACT AUDIT REPORT

for

INSTADAPP LABS

Prepared By: Shuxiao Wang

PeckShield
March 16, 2021

Document Properties

Client	InstaDApp Labs
Title	Smart Contract Audit Report
Target	DSAv2
Version	1.0
Author	Xuxian Jiang
Auditors	Huaguo Shi, Xuxian Jiang
Reviewed by	Jeff Liu
Approved by	Xuxian Jiang
Classification	Public

Version Info

Version	Date	Author(s)	Description
1.0	March 16, 2021	Xuxian Jiang	Final Release
0.2	March 12, 2021	Xuxian Jiang	Additional Findings #1
0.1	March 9, 2021	Xuxian Jiang	Initial Draft

Contact

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

Name	Shuxiao Wang
Phone	+86 173 6454 5338
Email	contact@peckshield.com

Contents

1 Introduction

Given the opportunity to review the design document and related smart contract source code of the `InstaDApp DeFi Smart Accounts` version 2 (or `DSAv2`), 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 DSAv2

`InstaDApp` is a popular DeFi portal that aggregates the major protocols using a smart wallet layer and bridge contracts, making it easy for users to make the best decisions about assets and execute previously complex transactions seamlessly. This upgrade to `DSAv2` provides a number of enhancements, including a generic extensible implementation framework, a user-facing account proxy, as well as new connectors design.

The basic information of DSAv2 is as follows:

Table 1.1: Basic Information of DSAv2

Item	Description
Issuer	InstaDApp Labs
Website	https://instadapp.io/
Type	Ethereum Smart Contract
Platform	Solidity
Audit Method	Whitebox
Latest Audit Report	March 16, 2021

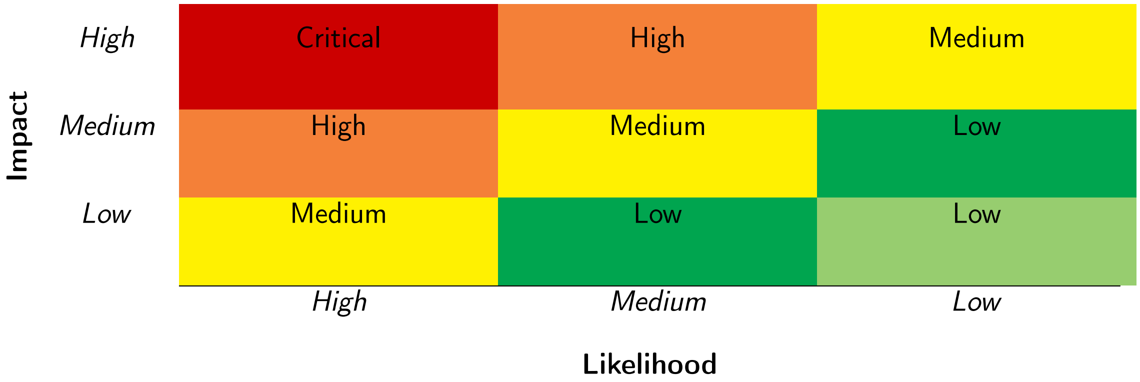
In the following, we show the Git repository of reviewed files and the commit hash value used in this audit:

- https://github.com/InstaDApp/dsa-contracts (83d3f9de)

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. Moreover, in case there is an issue that may affect an active protocol that has been deployed, the public version of this report may omit such issue, but will be amended with full details right after the affected protocol is upgraded with respective fixes.

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 DSAv2 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		
Medium	1	🟦
Low	1	🟦
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 1 medium-severity vulnerability, and 1 low-severity vulnerability.

Table 2.1: Key Audit Findings

ID	Severity	Title	Category	Status
PVE-001	Low	Improved Sanity Checks Of Function Parameters	Coding Practices	Confirmed
PVE-002	Medium	Management of Privileged Master Account	Security Features	Mitigated

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 Improved Sanity Checks Of Function Parameters

- ID: PVE-001
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: `InstaConnectorsV2`
- Category: Coding Practices [4]
- CWE subcategory: CWE-1126 [1]

Description

DeFi protocols typically have a number of system-wide settings or parameters that can be dynamically configured on demand. The `DSAv2` smart accounts are no exception. Specifically, if we examine the `InstaConnectorsV2` contract, it has defined a number of protocol-wide configurations, e.g., `chief` and `connectors`. In the following, we show a specific routine `updateConnectors()` that is designed to update connectors that provide the functionalities or features to enhance smart accounts.

```
    /**
     * @dev Update Connectors
     * @param _connectorNames Array of Connector Names.
     * @param _connectors Array of Connector Address.
    */
    function updateConnectors(string[] calldata _connectorNames, address[] calldata _connectors) external isChief {
        for (uint i = 0; i < _connectors.length; i++) {
            require(connectors[_connectorNames[i]] != address(0), "addConnectors: _connectorName not added to update");
            require(_connectors[i] != address(0), "addConnectors: _connector address is not vaild");
            ConnectorInterface(_connectors[i]).name(); // Checking if connector has function name()
            emit LogConnectorUpdated(_connectorNames[i], connectors[_connectorNames[i]], _connectors[i]);
            connectors[_connectorNames[i]] = _connectors[i];
        }
```

```
83    }
```

Listing 3.1: InstaConnectorsV2::updateConnectors()

Our result shows the update logic on the above logic can be improved by applying more rigorous sanity checks. Specifically, this routine essentially iterates the given `connectors` and updates the internal connector mapping (line 81). Within the routine, it properly validates the given arguments in ensuring the validity of each connector. However, it misses the validation on the length of the given arguments, i.e., `require(_connectors.length == _connectors.length, "updateConnectors: not same length")`.

Recommendation Properly validate the given two arguments to `updateConnectors()` have the same length.

Status The issue has been confirmed.

3.2 Management of Privileged Master Account

- ID: PVE-002
- Severity: Medium
- Likelihood: Medium
- Impact: Medium
- Target: `Multiple Contracts`
- Category: Security Features [3]
- CWE subcategory: CWE-287 [2]

Description

Following the same design as the first version, `DSAv2` has a privileged account `master` that plays a critical role in governing and regulating the system-wide operations (e.g., `connector` registration, `implementation` customization, and parameter setting). The configured connectors also have the privilege to control or govern the flow of user assets managed in these smart accounts.

With great privilege comes great responsibility. Our analysis shows that the `master` account is indeed privileged. To elaborate, we show below one guarded function `addConnectors()`. As the name indicates, this function allows for the additions of new connectors. These connectors are allowed to execute the code in the context of users' smart accounts (via `delegatecall()`), effectively accessing and managing any asserts held in these smart accounts.

```
    /**
     * @dev Add Connectors
     * @param _connectorNames Array of Connector Names.
     * @param _connectors Array of Connector Address.
    */
    function addConnectors(string[] calldata _connectorNames, address[] calldata
        _connectors) external isChief {
```

```
        require(_connectors.length == _connectors.length, "addConnectors: not same length");
        for (uint i = 0; i < _connectors.length; i++) {
            require(connectors[_connectorNames[i]] == address(0), "addConnectors: _connectorName added already");
            require(_connectors[i] != address(0), "addConnectors: _connectors address not vaild");
            ConnectorInterface(_connectors[i]).name(); // Checking if connector has function name()
            connectors[_connectorNames[i]] = _connectors[i];
            emit LogConnectorAdded(_connectorNames[i], _connectors[i]);
        }
    }
```

Listing 3.2: InstaConnectorsV2::addConnectors()

We emphasize that this privileged account is necessary and this account should not be managed by a normal `EOA` account. In fact, it is better governed by a `DAO`-like structure. The discussion with the team has confirmed that the `master` account will be managed by DAO. We point out that a compromised `master` account would allow the attacker to add a malicious `connector` to steal funds in these smart accounts.

Recommendation Promptly transfer the `master` privilege to the intended `DAO`-like governance contract. Any changes can also be mitigated with a timelock-based mechanism. Moreover, 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 mitigated with the planned DAO-based governance to regulate the `master` privileges.

3.3 Other Suggestions

Due to the fact that compiler upgrades might bring unexpected compatibility or inter-version consistencies, it is always suggested to use fixed compiler versions whenever possible. As an example, we highly encourage to explicitly indicate the Solidity compiler version, e.g., `pragma solidity 0.7.0;` instead of `pragma solidity ^0.7.0;`.

Moreover, we strongly suggest not to use experimental Solidity features or third-party unaudited libraries. If necessary, refactor current code base to only use stable features or trusted libraries. In case there is an absolute need of leveraging experimental features or integrating external libraries, make necessary contingency plans.

4 Conclusion

In this audit, we have analyzed the DSAv2 documentation and implementation. The audited system does involve various intricacies in both design and implementation. The current code base is well organized and 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.