A&D FORENSICS

SMART CONTRACT AUDIT

For

REDSWAN®

Prepared by: A&D Forensics

contactus@adforensics.com.ng

July, 2022

AUDIT REPORT 2022

TABLE OF CONTENTS

OVERVIEW 6

Project Summary 6

Audit Summary 6

Vulnerability Summary 6

Audit Scope 7

FINDINGS 8

Project Description 8

Project Structure 8

Automated Test using Cargo 8

Manual Test Comparing to SPL 9

Others 16

CONCLUSION 17

Overview 17

Problems and Recommendation 17

DISCLAIMER 18

INTRODUCTION

On May 18, 2022, RedSwan contracted A&D Forensics to conduct an audit on SWAN Token on Solana Blockchain. We detailed our methodology in this report to evaluate potential security issues in the smart contract and stated our observations in this report. With this report, we have tried to ensure the reliability and correctness of their smart contract by complete and rigorous assessment of their system's architecture and the smart contract codebase and associated libraries.

ABSTRACT

This report has been prepared for Custom Solana Program Library named SWAN to discover issues and vulnerabilities in the source code of Swan Token forked from spl that were not part an officially recognized library. A comprehensive examination has been performed, utilizing Tooling Analysis and Manual Review techniques by smart contract security expert.

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 general specifications and intentions of the standard design patterns
- Cross referencing contract structure and implementation against similar contract produced by industry leaders.
- Through 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 perspectives:

- Enhancing 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.

OVERVIEW

Project Summary

Project Name	**Swan Token**
Platform	**Solana**
Codebase	**https://github.com/nerdCross/update**
Commit	**b34f897f151c691cdb132348b656cf29592e2284**

Audit Summary

Delivery Date	July 14, 2022
Audit Methodology	Static Analysis, Manual Review
Key Components	

Vulnerability Summary

Vulnerability Level	Total	Pending	Acknowledged	Partially Resolved	Resolved
Critical	0	0	0	0	0
Major	4				4
Medium	0	0	0	0	0

Vulnerability Level	Total	Pending	Acknowledged	Partially Resolved	Resolved
Minor	3		3		
Informational	0	0	0	0	0
Discussion	0	0	0	0	0

Audit Scope

Cluster	Testnet
Mint Address	GoPPB2Hj9uCfgCf5divtF9MeeD1zhdkgfJvWob7udvt7

FINDINGS

Project Description

A token program which is forked from Solana Program Library, usable for fungible and non-fungible tokens.

This program provides an interface and implementation that third parties can utilize to create and use SWAN tokens.

Automated Test Using Cargo

- cargo test

  It allows to run the host-based tests.

  All passed.

  There is no compiling errors or issues.

- cargo test-bpf

  It allows BPF program tests.

  All passed.

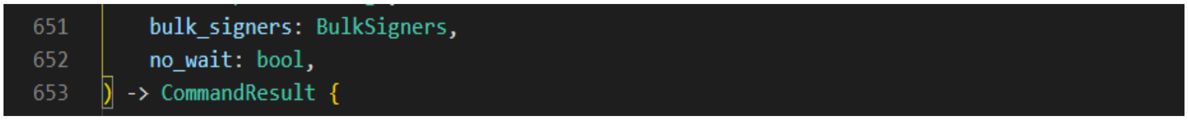
  There is no compiling errors or issues.

Manual Test Comparing to SPL

- cli

  1. Missing “allow_non_system_account_recipient” parameter in row 653 of main.rs

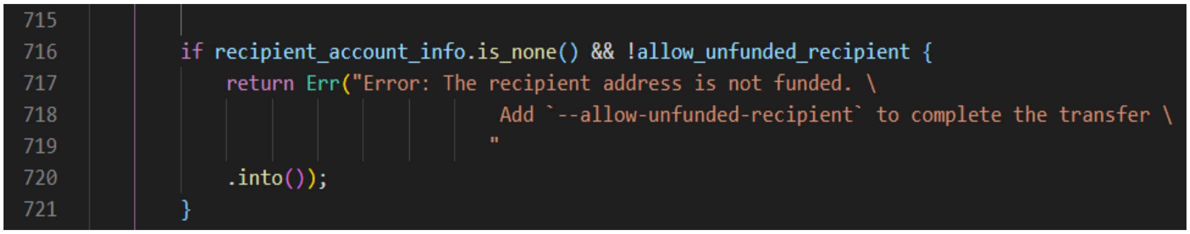
     [Major Issue] - Resolved ✓



```
651     bulk_signers: BulkSigners,
652     no_wait: bool,
653 ) -> CommandResult {
```

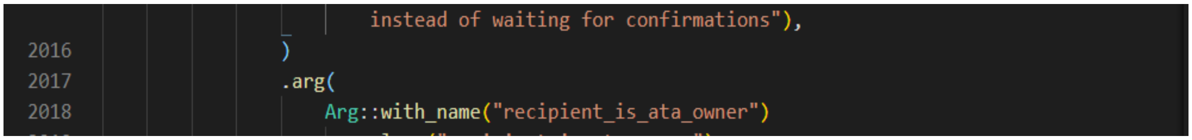
  2. Missing “recipient_is_system_account” assertion in row 715 of main.rs

     [Major Issue] - Resolved ✓



```
715
716         if recipient_account_info.is_none() && !allow_unfunded_recipient {
717             return Err("Error: The recipient address is not funded. \
718                                     Add `--allow-unfunded-recipient` to complete the transfer \
719                                    "
720             .into());
721         }
```

3. Missing “allow_non_system_account_recepient” assertion in row 2017 of main.rs [Major Issue] - Resolved ✓



```
                        instead of waiting for confirmations"),
2016            )
2017            .arg(
2018                Arg::with_name("recipient_is_ata_owner")
```

4. Missing tests module in main.rs [Major Issue] - Resolved ✓

- js

  No issue found.

- program

  No issue found.

- program-2022

  1. Missing immutable_owner module in src/extension [Minor Issue] - Acknowledged

     It is the module for Indicating that the Account owner authority cannot be changed

  2. Missing non_transferable module in src/extension [Minor Issue] - Acknowledged

     It is the module for Indicating that the tokens from this mint can't be transferred

     Not implemented immutable_owner and non_transferable module in src/instruction.rs [Minor Issue] - Acknowledged

- rust

  No issue found

- ts

  No issue found

- others

  1. Missing program-2022-test module. [Major Issue] - Resolved

  Should be done SPL-Token 2022 Integration Tests.

  Recommendation: Refer to latest spl token program tests.

Others

- Hardcoded Addresses

  Not found

- Honeypot Leak

  Not found

CONCLUSION

Overall Design

- Good project architecture and implemented spl token program standard requirements.

Problems

- Missing some assertions and not implemented extensible option modules.
  It could cause some unexpected results or inconvenience implementation in the future.
  Recommendation: Refer to the latest spl token program and implement missing features.

DISCLAIMER

This report is not an endorsement or indictment of any particular project or team, and the report does not guarantee the security of any particular project. Therefore, should not be interpreted as having any bearing on, the potential economics of a token, token sale or any other product, service or other asset.

In addition, this report does not provide any warranty or representation to any Third-Party in any respect, including regarding the bug-free nature of code, the business model or proprietors of any such business model, and the legal compliance of any such business. Hence, no third party should rely on this report in any way, including for the purpose of making any decisions to buy or sell any token, product, service or other asset.

Specifically, for the avoidance of doubt, this report does not constitute investment advice. Hence, it is not intended to be relied upon as investment advice, an endorsement of this project or team, and it is not a guarantee as to the absolute security of the project as the scope of our review is limited to the token module of the solana-cli residing at the specific address. We owe no duty to any Third-Party by virtue of publishing these Reports.

Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty.

CONTACT US

A&D Forensics

☎ +234 909 550 3040

www.adforensics.com.ng

✉ contactus@adforensics.com.ng

No 3. Rabat Street, Wuse Zone 6, FCT Abuja, Nigeria