Swap Smart Contract

April 2024

SMART CONTRACT AUDIT REPORT

ExVul

www.exvul.com

Table of Contents

1. EXECUTIVE SUMMARY

Exvul Web3 Security was engaged by Swap to review smart contract implementation. The assessment was conducted in accordance with our systematic approach to evaluate potential security issues based upon customer requirement. The report provides detailed recommendations to resolve the issue and provide additional suggestions or recommendations for improvement.

Low risk is mainly related to fees and privileged roles.

The outcome of the assessment outlined in chapter 3 provides the system's owners a full description of the vulnerabilities identified, the associated risk rating for each vulnerability, and detailed recommendations that will resolve the underlying technical issue.

1.1 Methodology

To standardize the evaluation, we define the following terminology based on OWASP Risk Rating Methodology [10] which is the gold standard in risk assessment using the following risk models:

- 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: determine the overall criticality of the risk.

Likelihood can be: High, Medium and Low and impact are categorized into for: High, Medium, Low, Informational. Severity is determined by likelihood and impact and can be classified into five categories accordingly, Critical, High, Medium, Low, Informational shown in table 1.1.

Likelihood				
High	***Informational***	**Medium**	**High**	**Critical**
Medium	***Informational***	**Low**	**Medium**	**High**
Low	***Informational***	**Low**	**Low**	**Medium**
	Informational	***Low***	***Medium***	***High***
	IMPACT			

Table 1.1 Overall Risk Severity

To evaluate the risk, we will be going through a list of items, and each would be labelled with a severity category. The audit was performed with a systematic approach guided by a comprehensive assessment list carefully designed to identify known and impactful security issues. If our tool or analysis does not identify any issue, the contract can be considered safe regarding the assessed item. For any discovered issue, we might further deploy contracts on our private test environment 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 1.2.

- 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.
- Code and business security testing: 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.

Category	Assessment Item
Basic Coding Assessment	Apply Verification Control
	Authorization Access Control
	Forged Transfer Vulnerability
	Forged Transfer Notification
	Numeric Overflow
	Transaction Rollback Attack
	Transaction Block Stuffing Attack
	Soft Fail Attack
	Hard Fail Attack
	Abnormal Memo
	Abnormal Resource Consumption
	Secure Random Number
Advanced Source Code Scrutiny	Asset Security
	Cryptography Security
	Business Logic Review
	Source Code Functional Verification
	Account Authorization Control
	Sensitive Information Disclosure
	Circuit Breaker
	Blacklist Control
	System API Call Analysis
	Contract Deployment Consistency Check
	Semantic Consistency Checks

Category	Assessment Item
Additional Recommendations	Following Other Best Practices

Table 1.2: The Full List of Assessment Items

To better describe each issue we identified, we categorize the findings with Common Weakness Enumeration (CWE-699) [14], which is a community-developed list of software weakness types to better delineate and organize weaknesses around concepts frequently encountered in software development.

2. FINDINGS OVERVIEW

2.1 Project Info And Contract Address

Project Name: Swap

Audit Time: March 28nd, 2024 – April 8th, 2024

Language: Rust

File Name	Link
lib.rs	https://github.com/bitkeepwallet/solana-swap/bkswap/programs/raydium_extra_router/src/
mod.rs	https://github.com/bitkeepwallet/solana-swap/bkswap/programs/raydium_extra_router/src/instructions
route_swap_in.rs	https://github.com/bitkeepwallet/solana-swap/bkswap/programs/raydium_extra_router/src/instructions
swap_base_out.rs	https://github.com/bitkeepwallet/solana-swap/bkswap/programs/raydium_extra_router/src/instructions

2.2 Summary

Severity	Found	
Critical	0	
High	0	
Medium	0	
Low	2	🟦🟦
Informational	2	🟩🟩

2.3 Key Findings

Low risk is mainly related to fees and privileged roles.

ID	Severity	Findings Title	Status	Confirm
NVE-001	Low	Fee collection may be bypassed	Ignored	Confirmed
NVE-002	Low	Privileged roles can suspend contracts	Unconfirmed fixed(See the notes)	Confirmed
NVE-003	Informational	External interfaces may be risky	Unconfirmed fixed(See the notes)	Confirmed
NVE-004	Informational	It is not determined whether the redemption quantity is valid	Ignored	Confirmed

Table 2.3: Key Audit Findings

3. DETAILED DESCRIPTION OF FINDINGS

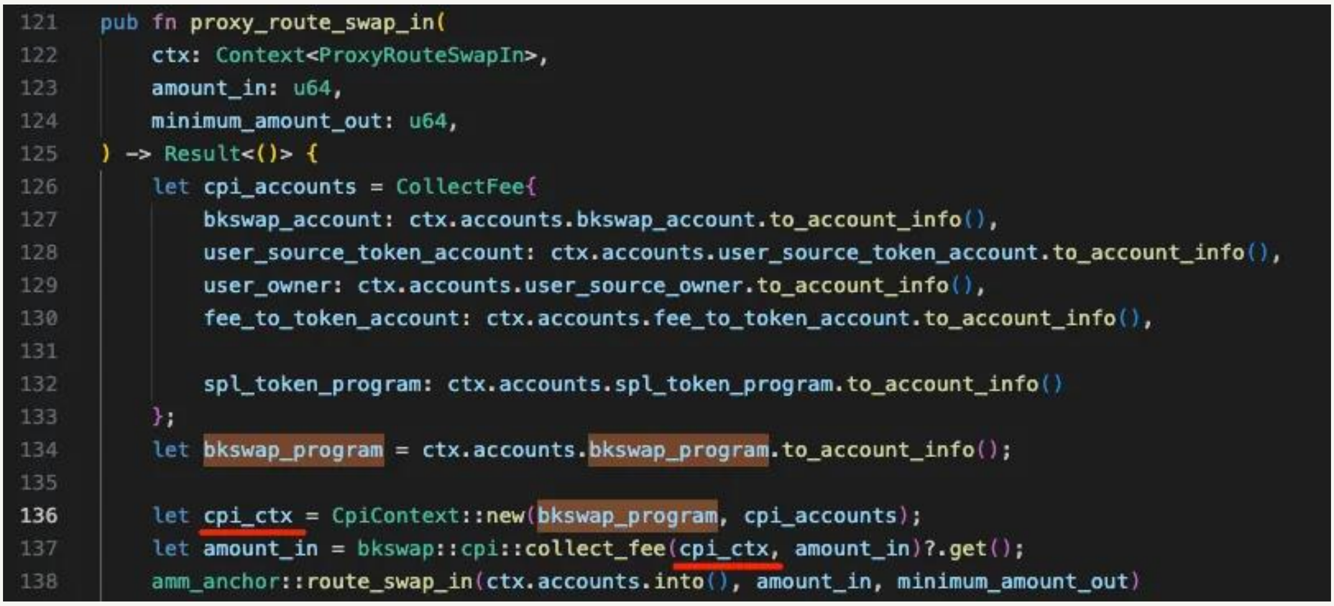
3.1 Fee collection may be bypassed

ID:	NVE-001	**Location:**	route_swap_in.rs
Severity:	Low	**Category:**	Business Issues
Likelihood:	Low	**Impact:**	Low

- route_swap_in.rs

Description:

bkswap_program is obtained through ctx.accounts.bkswap_program.to_account_info(), which means that the value of bkswap_program is determined by the account information passed to the transaction. If the caller forges bkswap_program, the handling fee collection will be bypassed.



```rust
pub fn proxy_route_swap_in(
    ctx: Context<ProxyRouteSwapIn>,
    amount_in: u64,
    minimum_amount_out: u64,
) -> Result<()> {
    let cpi_accounts = CollectFee{
        bkswap_account: ctx.accounts.bkswap_account.to_account_info(),
        user_source_token_account: ctx.accounts.user_source_token_account.to_account_info(),
        user_owner: ctx.accounts.user_source_owner.to_account_info(),
        fee_to_token_account: ctx.accounts.fee_to_token_account.to_account_info(),

        spl_token_program: ctx.accounts.spl_token_program.to_account_info()
    };
    let bkswap_program = ctx.accounts.bkswap_program.to_account_info();

    let cpi_ctx = CpiContext::new(bkswap_program, cpi_accounts);
    let amount_in = bkswap::cpi::collect_fee(cpi_ctx, amount_in)?.get();
    amm_anchor::route_swap_in(ctx.accounts.into(), amount_in, minimum_amount_out)
```

Figure 3.1.1 route_swap_in.rs

Recommendations:

Exvul Web3 Security recommends adding bkswap_program verification to ensure that the contract logic only allows expected bkswap_program calls.

Result: Confirmed

Fix Result:

Swap replied: Ordinary users cannot bypass it and cannot circumvent other people's fork status. If route_swap_in uses our contract and bkswap_program uses other contracts, we have no loss and it does not matter in this use case.

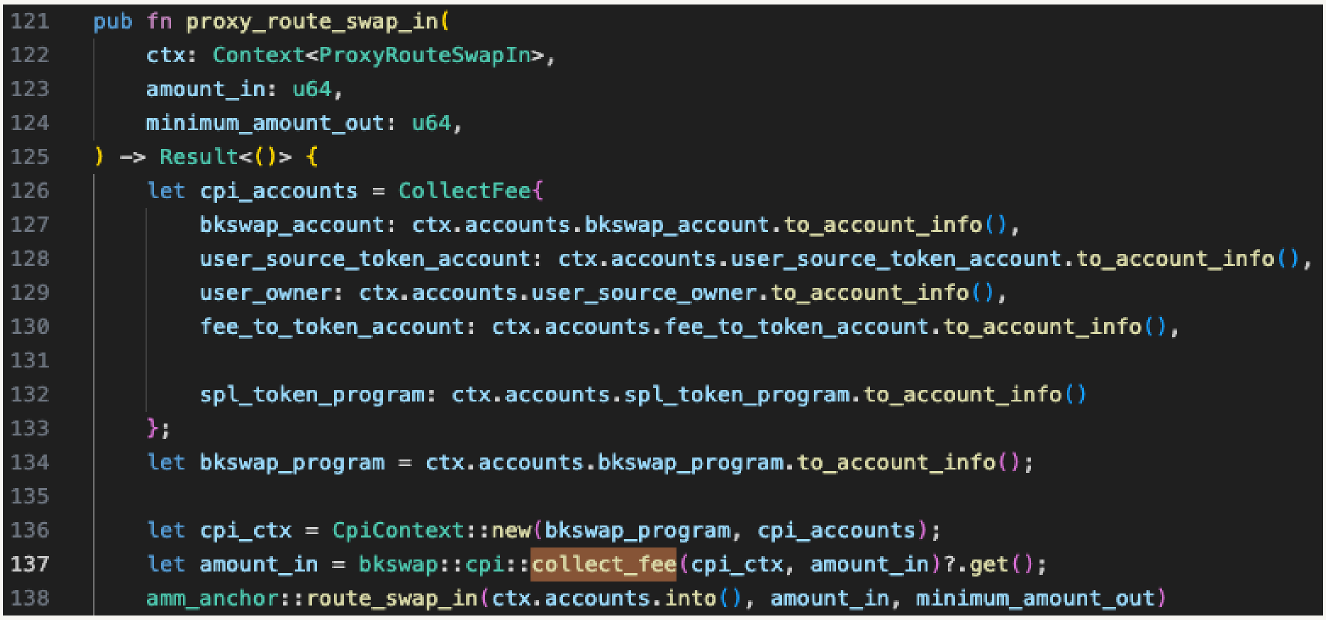
3.2 Privileged roles can suspend contracts

ID:	NVE-002	**Location:**	route_swap_in.rs
Severity:	Low	**Category:**	Business Issues
Likelihood:	Low	**Impact:**	Low

➢ route_swap_in.rs

Description:

When the proxy_route_swap_in method is redeemed, the collect_fee method is called to collect the handling fee. There is a pause mechanism is_paused in the collect_fee method. This variable is set by the authority manager in bkswap_account. If the manager is manipulated to cause malicious settings, the contract will become unusable.



```rust
pub fn proxy_route_swap_in(
    ctx: Context<ProxyRouteSwapIn>,
    amount_in: u64,
    minimum_amount_out: u64,
) -> Result<()> {
    let cpi_accounts = CollectFee{
        bkswap_account: ctx.accounts.bkswap_account.to_account_info(),
        user_source_token_account: ctx.accounts.user_source_token_account.to_account_info(),
        user_owner: ctx.accounts.user_source_owner.to_account_info(),
        fee_to_token_account: ctx.accounts.fee_to_token_account.to_account_info(),

        spl_token_program: ctx.accounts.spl_token_program.to_account_info()
    };
    let bkswap_program = ctx.accounts.bkswap_program.to_account_info();

    let cpi_ctx = CpiContext::new(bkswap_program, cpi_accounts);
    let amount_in = bkswap::cpi::collect_fee(cpi_ctx, amount_in)?.get();
    amm_anchor::route_swap_in(ctx.accounts.into(), amount_in, minimum_amount_out)
```

Figure 3.2.1 route_swap_in.rs

Recommendations:

Exvul Web3 Security recommends that privileged roles use multi-signature management to avoid malicious control.

Result: Confirmed

Fix Result:

Swap replied: The required management functions will be upgraded to multi-signature management in the future.

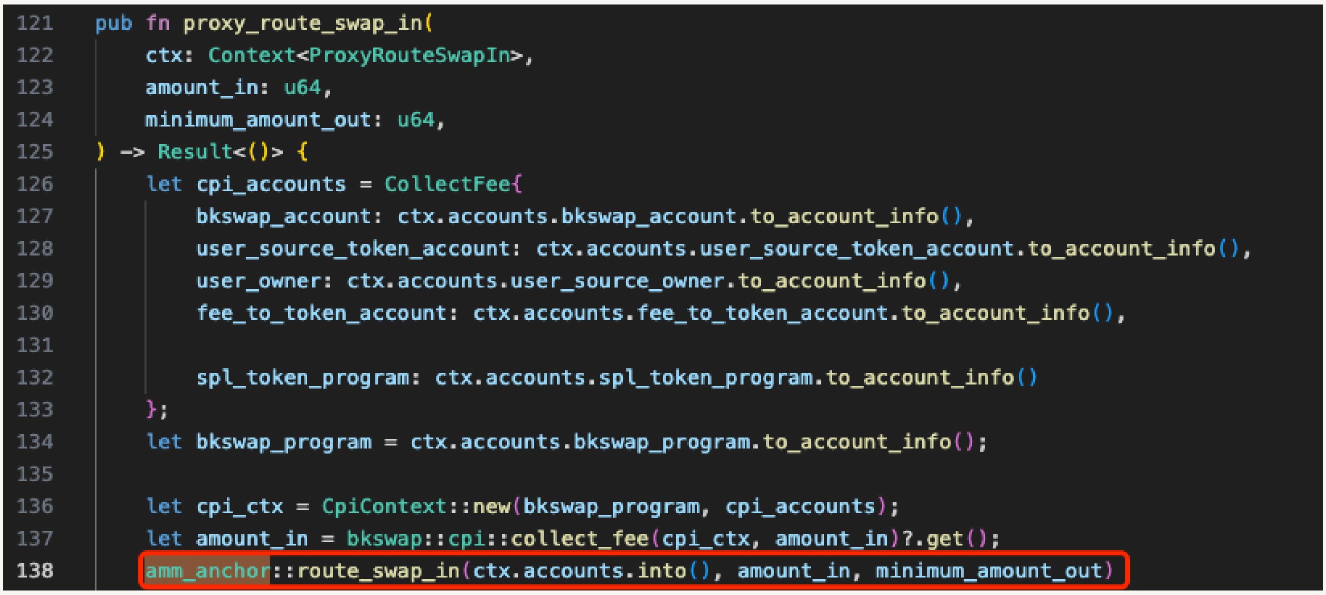
3.3 External interfaces may be risky

ID:	NVE-003	**Location:**	route_swap_in.rs
Severity:	Informational	**Category:**	Business Issues
Likelihood:	Low	**Impact:**	Informational

➢ route_swap_in.rs

Description:

The proxy_route_swap_in method uses the Raydium Protocol external interface when exchanging. If security risks occur when exchanging the external interface, the contract may also have varying degrees of risks.



```
pub fn proxy_route_swap_in(
    ctx: Context<ProxyRouteSwapIn>,
    amount_in: u64,
    minimum_amount_out: u64,
) -> Result<()> {
    let cpi_accounts = CollectFee{
        bkswap_account: ctx.accounts.bkswap_account.to_account_info(),
        user_source_token_account: ctx.accounts.user_source_token_account.to_account_info(),
        user_owner: ctx.accounts.user_source_owner.to_account_info(),
        fee_to_token_account: ctx.accounts.fee_to_token_account.to_account_info(),

        spl_token_program: ctx.accounts.spl_token_program.to_account_info()
    };
    let bkswap_program = ctx.accounts.bkswap_program.to_account_info();

    let cpi_ctx = CpiContext::new(bkswap_program, cpi_accounts);
    let amount_in = bkswap::cpi::collect_fee(cpi_ctx, amount_in)?.get();
    amm_anchor::route_swap_in(ctx.accounts.into(), amount_in, minimum_amount_out)
```

Figure 3.3.1 route_swap_in.rs

Recommendations:

Exvul Web3 Security recommends: There is currently a suspension mechanism in the contract, which can alleviate external interface security risks, but multi-signature administrators are required to manage the suspension mechanism to avoid improper use of the suspension mechanism.

Result: Confirmed

Fix Result:
Swap replied: The required management functions will be upgraded to multi-signature management in the future.

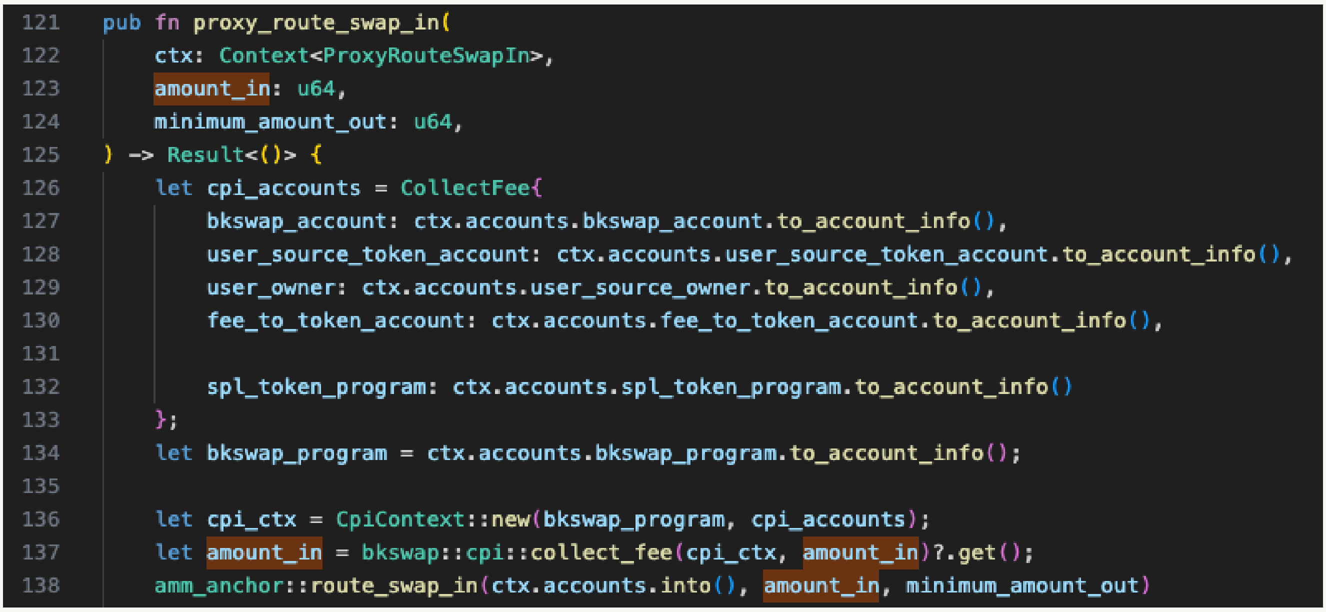
3.4 It is not determined whether the redemption quantity is valid

ID:	NVE-004	**Location:**	route_swap_in.rs
Severity:	Informational	**Category:**	Business Issues
Likelihood:	Low	**Impact:**	Informational

- route_swap_in.rs

Description:

The proxy_route_swap_in method is used to exchange funds. This method does not determine whether the input parameter amount_in is zero, which will lead to a zero-value exchange. At the same time, no handling fee will be charged, and an invalid transfer call will be executed.



```rust
pub fn proxy_route_swap_in(
    ctx: Context<ProxyRouteSwapIn>,
    amount_in: u64,
    minimum_amount_out: u64,
) -> Result<()> {
    let cpi_accounts = CollectFee{
        bkswap_account: ctx.accounts.bkswap_account.to_account_info(),
        user_source_token_account: ctx.accounts.user_source_token_account.to_account_info(),
        user_owner: ctx.accounts.user_source_owner.to_account_info(),
        fee_to_token_account: ctx.accounts.fee_to_token_account.to_account_info(),

        spl_token_program: ctx.accounts.spl_token_program.to_account_info()
    };
    let bkswap_program = ctx.accounts.bkswap_program.to_account_info();

    let cpi_ctx = CpiContext::new(bkswap_program, cpi_accounts);
    let amount_in = bkswap::cpi::collect_fee(cpi_ctx, amount_in)?.get();
    amm_anchor::route_swap_in(ctx.accounts.into(), amount_in, minimum_amount_out)
```

Figure 3.4.1 route_swap_in.rs

Recommendations:

Exvul Web3 Security recommends checking for zero-valued inputs in methods to avoid invalid transfer calls.

Result: Confirmed

Fix Result:

Swap replied: According to other project development habits, zero value checking is not added.

4. CONCLUSION

In this audit, we thoroughly analyzed **Swap** smart contract implementation. The problems found are described and explained in detail in Section 3. The problems found in the audit have been communicated to the project leader. We therefore consider the audit result to be **PASSED**. To improve this report, we greatly appreciate any constructive feedbacks or suggestions, on our methodology, audit findings, or potential gaps in scope/coverage.

5. APPENDIX

5.1 Basic Coding Assessment

5.1.1 Apply Verification Control

- Description: The security of apply verification
- Result: Not found
- Severity: Critical

5.1.2 Authorization Access Control

- Description: Permission checks for external integral functions
- Result: Not found
- Severity: Critical

5.1.3 Forged Transfer Vulnerability

- Description: Assess whether there is a forged transfer notification vulnerability in the contract
- Result: Not found
- Severity: Critical

5.1.4 Transaction Rollback Attack

- Description: Assess whether there is transaction rollback attack vulnerability in the contract.
- Result: Not found
- Severity: Critical

5.1.5 Transaction Block Stuffing Attack

- Description: Assess whether there is transaction blocking attack vulnerability.
- Result: Not found
- Severity: Critical

5.1.6 Soft Fail Attack Assessment

- Description: Assess whether there is soft fail attack vulnerability.
- Result: Not found
- Severity: Critical

5.1.7 Hard Fail Attack Assessment

- Description: Examine for hard fail attack vulnerability
- Result: Not found
- Severity: Critical

5.1.8 Abnormal Memo Assessment

- Description: Assess whether there is abnormal memo vulnerability in the contract.
- Result: Not found
- Severity: Critical

5.1.9 Abnormal Resource Consumption

- Description: Examine whether abnormal resource consumption in contract processing.
- Result: Not found
- Severity: Critical

5.1.10 Random Number Security

- Description: Examine whether the code uses insecure random number.
- Result: Not found
- Severity: Critical

5.2 Advanced Code Scrutiny

5.2.1 Cryptography Security

- Description: Examine for weakness in cryptograph implementation.
- Results: Not Found
- Severity: High

5.2.2 Account Permission Control

- Description: Examine permission control issue in the contract
- Results: Not Found
- Severity: Medium

5.2.3 Malicious Code Behavior

- Description: Examine whether sensitive behavior present in the code
- Results: Not found
- Severity: Medium

5.2.4 Sensitive Information Disclosure

- Description: Examine whether sensitive information disclosure issue present in the code.
- Result: Not found
- Severity: Medium

5.2.5 System API

- Description: Examine whether system API application issue present in the code
- Results: Not found
- Severity: Low

6. DISCLAIMER

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 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 without ExVul's prior written consent.

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 ExVul 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. ExVul's position is that each company and individual are responsible for their own due diligence and continuous security. ExVul'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.

7. REFERENCES

[1] MITRE. CWE- 191: Integer Underflow (Wrap or Wraparound).

https://cwe.mitre.org/data/ definitions/191.html.

[2] MITRE. CWE- 197: Numeric Truncation Error.

https://cwe.mitre.org/data/definitions/197. html.

[3] MITRE. CWE-400: Uncontrolled Resource Consumption.

https://cwe.mitre.org/data/ definitions/400.html.

[4] MITRE. CWE-440: Expected Behavior Violation.

https://cwe.mitre.org/data/definitions/440. html.

[5] MITRE. CWE-684: Protection Mechanism Failure.

https://cwe.mitre.org/data/definitions/ 693.html.

[6] MITRE. CWE CATEGORY: 7PK - Security Features.

https://cwe.mitre.org/data/definitions/ 254.html.

[7] MITRE. CWE CATEGORY: Behavioral Problems.

https://cwe.mitre.org/data/definitions/438. html.

[8] MITRE. CWE CATEGORY: Numeric Errors.

https://cwe.mitre.org/data/definitions/189.html.

[9] MITRE. CWE CATEGORY: Resource Management Errors.

https://cwe.mitre.org/data/ definitions/399.html.

[10] OWASP. Risk Rating Methodology.

https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

🌐 www.exvul.com

✉ contact@exvul.com

@EXVULSEC

github.com/EXVUL-Sec

ExVul