Bitget Swap Smart Contract

SMART CONTRACT AUDIT REPORT

October 2024

ExVul

www.exvul.com

Table of Contents

1. EXECUTIVE SUMMARY

Exvul Web3 Security was engaged by Bitget 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.

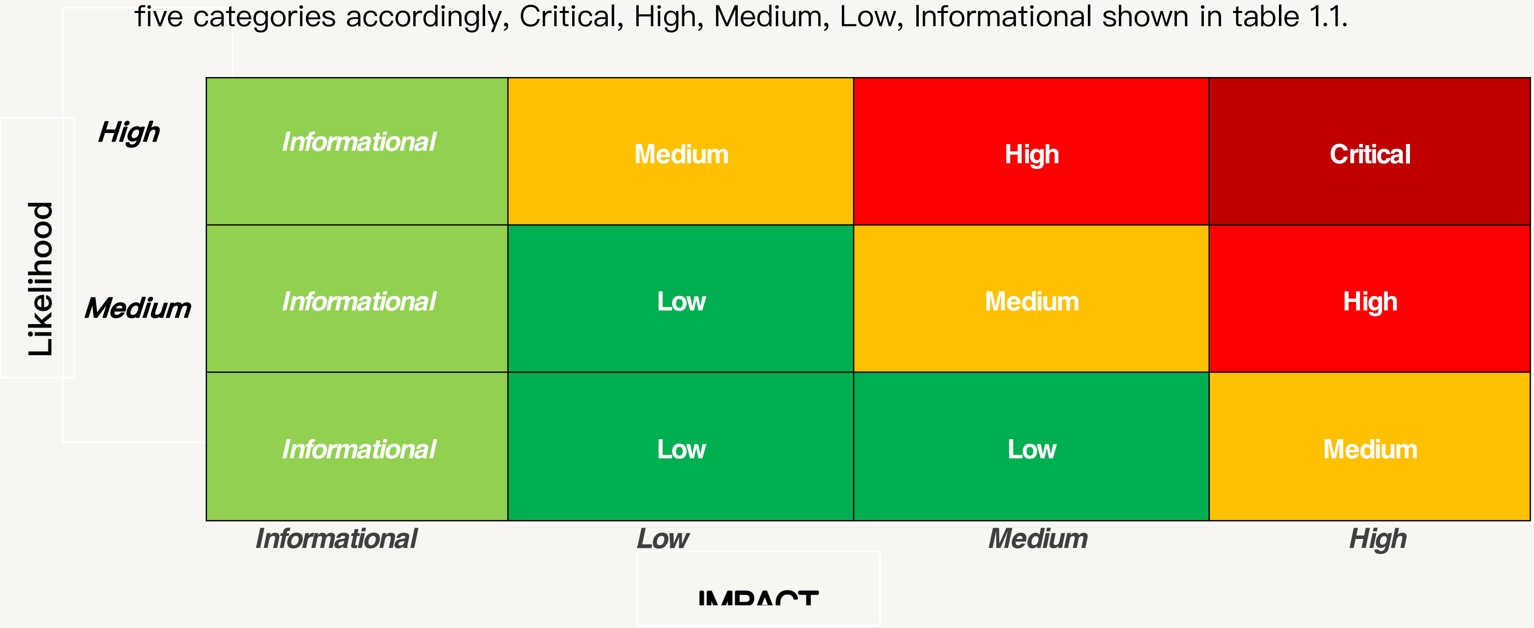
The outcome of the assessment outlined in chapter 3 provides the system's owners a full description of the vulnerabilities identified, the associated risk rating for each vulnerability, and detailed recommendations that will resolve the underlying technical issue.

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
	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

Category	Assessment Item
	Source Code Functional Verification
	Account Authorization Control
	Sensitive Information Disclosure
	Circuit Breaker
	Blacklist Control
	System API Call Analysis
	Contract Deployment Consistency Check
Additional Recommendations	Semantic Consistency Checks
	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: bitget-swap

Audit Time: October 18, 2024 — October 25, 2024

Language: Rust

File Name	Link
bitget-swap	https://github.com/bitgetwallet/solana-swap/commit/0d93627476d537f45fcc8d5f2069bbf82139a6b7

2.2 Summary

Severity	Found	
Critical	0	
High	0	
Medium	1	🟨
Low	5	🟦🟦🟦🟦🟦
Informational	0	

2.3 Key Findings

ID	Severity	Findings Title	Status	Confirm
NVE–001	Medium	Does not make reasonable judgments on multiple parameters during initialization	Fixed	Confirmed
NVE–002	Low	SetAuthority Make sure the old and new authorities are inconsistent	Fixed	Confirmed
NVE–003	Low	SetAuthority Ensure that the new authority cannot be zero	Fixed	Confirmed
NVE–004	Low	Should ensure that bal is greater than rent_balance	Fixed	Confirmed
NVE–005	Low	Authority may be set to an empty address when initialized	Fixed	Confirmed
NVE–006	Low	Allowlist should check users count	Fixed	Confirmed

Table 2.3: Key Audit Findings

3. DETAILED DESCRIPTION OF FINDINGS

3.1 Does not make reasonable judgments on multiple parameters during initialization

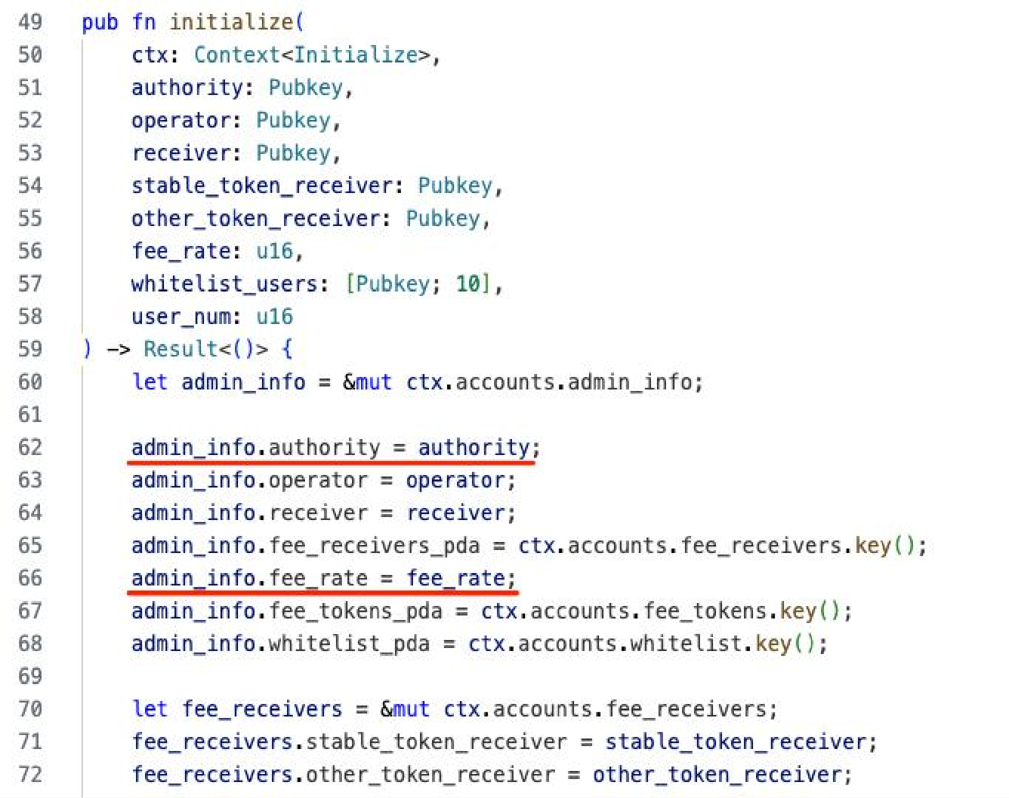
ID:	NVE-001	**Location:**	initialize.rs
Severity:	Medium	**Category:**	Business Issues
Likelihood:	Low	**Impact:**	High

Description:

Initialize admin_info fee_rate = fee_rate; and admin_info authority = authority, fee_rate rate setting has a maximum limit in the set_fee_rate method, but no limit at initialization

The authority privileged role should set a normal address during initialization. If the authority is set to an empty address during initialization, subsequent authority permissions will not be able to be used normally.

It is recommended that the maximum limit fee_rate set during initialization; the authority privileged role limit cannot be an empty address.



```rust
pub fn initialize(
    ctx: Context<Initialize>,
    authority: Pubkey,
    operator: Pubkey,
    receiver: Pubkey,
    stable_token_receiver: Pubkey,
    other_token_receiver: Pubkey,
    fee_rate: u16,
    whitelist_users: [Pubkey; 10],
    user_num: u16
) -> Result<()> {
    let admin_info = &mut ctx.accounts.admin_info;

    admin_info.authority = authority;
    admin_info.operator = operator;
    admin_info.receiver = receiver;
    admin_info.fee_receivers_pda = ctx.accounts.fee_receivers.key();
    admin_info.fee_rate = fee_rate;
    admin_info.fee_tokens_pda = ctx.accounts.fee_tokens.key();
    admin_info.whitelist_pda = ctx.accounts.whitelist.key();

    let fee_receivers = &mut ctx.accounts.fee_receivers;
    fee_receivers.stable_token_receiver = stable_token_receiver;
    fee_receivers.other_token_receiver = other_token_receiver;
```

Recommendations:

Exvul Web3 Security recommends add more checks.

Customer response:

To be added authority, operator, receiver, stable_token_receiverother_token_receiver not 0 address and fee_rate less than the maximum FEE_RATE check

Result: Confirmed

Fix Result: fixed

Customer response:

To be added authority, operator, receiver, stable_token_receiverother_token_receiver not 0 address and fee_rate less than the maximum FEE_RATE check

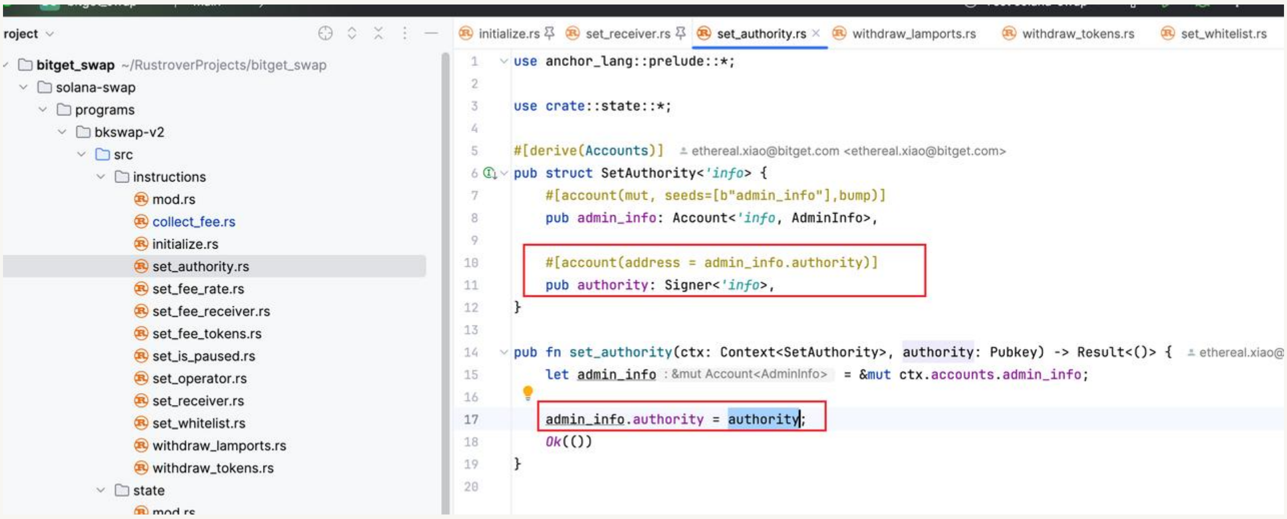
Fixed version: 89a6cd4ada6c8a6fcd84567a0bbc3c5a7daa36de

3.2 SetAuthority Make sure the old and new authorities are inconsistent

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

Description:

You can add an extra check.



```rust
use anchor_lang::prelude::*;

use crate::state::*;

#[derive(Accounts)]
pub struct SetAuthority<'info> {
    #[account(mut, seeds=[b"admin_info"],bump)]
    pub admin_info: Account<'info, AdminInfo>,

    #[account(address = admin_info.authority)]
    pub authority: Signer<'info>,
}

pub fn set_authority(ctx: Context<SetAuthority>, authority: Pubkey) -> Result<()> {
    let admin_info : &mut Account<AdminInfo> = &mut ctx.accounts.admin_info;

    admin_info.authority = authority;
    Ok(())
}
```

Recommendations:

Exvul Web3 Security recommends add extra check

Result: Confirmed

Fix Result: Fixed

Customer response:

Added, in the set_authority method of set_admin_infos.rs file

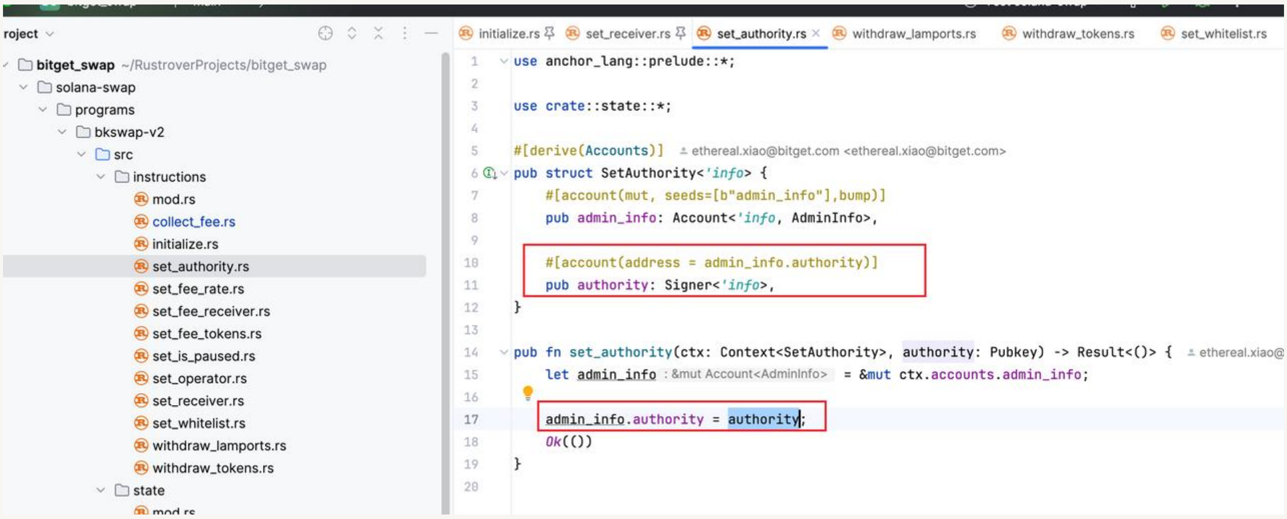
Fixed version: 89a6cd4ada6c8a6fcd84567a0bbc3c5a7daa36de

3.3 SetAuthority Ensure that the new authority cannot be zero

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

Description:

If the authority is set to an empty address, subsequent authority permissions will not be used normally. It is recommended to add a judgment that cannot be zero address



```rust
use anchor_lang::prelude::*;

use crate::state::*;

#[derive(Accounts)]
pub struct SetAuthority<'info> {
    #[account(mut, seeds=[b"admin_info"],bump)]
    pub admin_info: Account<'info, AdminInfo>,

    #[account(address = admin_info.authority)]
    pub authority: Signer<'info>,
}

pub fn set_authority(ctx: Context<SetAuthority>, authority: Pubkey) -> Result<()> {
    let admin_info = &mut ctx.accounts.admin_info;

    admin_info.authority = authority;
    Ok(())
}

```

Recommendations:

Exvul Web3 Security recommends

Result: Confirmed

Fix Result: fixed

Customer response: Added, in the set_authority method of set_admin_infos.rs file

Fixed version: 89a6cd4ada6c8a6fcd84567a0bbc3c5a7daa36de

3.4 Should ensure that bal is greater than rent_balance

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

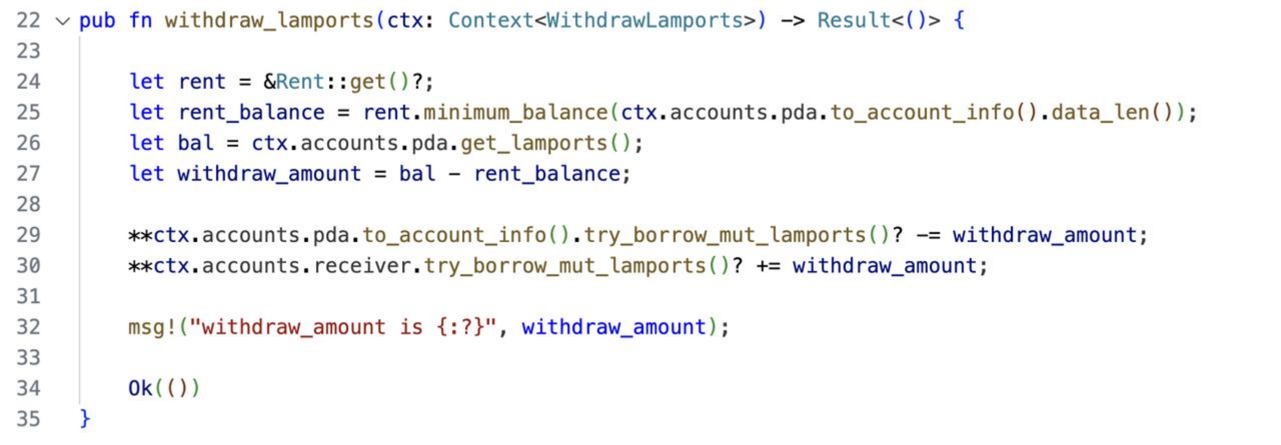
Description:

Location:

1.programs/bkswap-v2/src/instructions/withdraw_lamports.rs

2.programs/raydium-clmm-router/src/instructions/withdraw_lamports.rs

If the amount of data stored in the account increases, but the Lamports in the account do not increase accordingly; or if the Solana network rental rate increases, resulting in an increase in the required minimum balance. This may cause the bal to be less than rent_balance, resulting in calculation errors



```
pub fn withdraw_lamports(ctx: Context<WithdrawLamports>) -> Result<()> {

    let rent = &Rent::get()?;
    let rent_balance = rent.minimum_balance(ctx.accounts.pda.to_account_info().data_len());
    let bal = ctx.accounts.pda.get_lamports();
    let withdraw_amount = bal - rent_balance;

    **ctx.accounts.pda.to_account_info().try_borrow_mut_lamports()? -= withdraw_amount;
    **ctx.accounts.receiver.try_borrow_mut_lamports()? += withdraw_amount;

    msg!("withdraw_amount is {:?}", withdraw_amount);

    Ok(())
}
```

Recommendations:

Exvul Web3 Security recommends that

Result: Confirmed

Fix Result: fixed

Customer response: As suggested, add bal > = rent_balance check

Fixed version: 89a6cd4ada6c8a6fcd84567a0bbc3c5a7daa36de

3.5 Authority may be set to an empty address when initialized

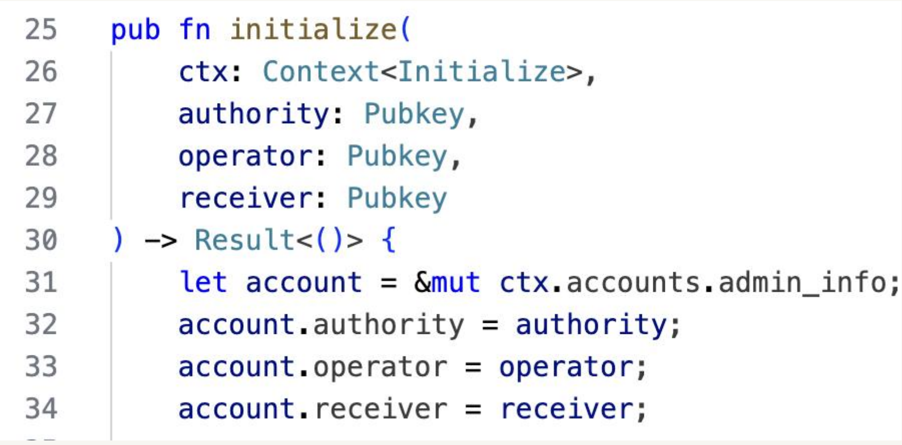
ID:	NVE-005	**Location:**	lib.rs
Severity:	Low	**Category:**	Business Issues
Likelihood:	Low	**Impact:**	Low

Description:

The authority privileged role should set a normal address during initialization. If the authority is set to an empty address during initialization, subsequent authority permissions will not be able to be used normally.

It is recommended that the authority privilege role restriction cannot be an empty address during initialization.

Fixed version: 89a6cd4ada6c8a6fcd84567a0bbc3c5a7daa36de



```rust
pub fn initialize(
    ctx: Context<Initialize>,
    authority: Pubkey,
    operator: Pubkey,
    receiver: Pubkey
) -> Result<()> {
    let account = &mut ctx.accounts.admin_info;
    account.authority = authority;
    account.operator = operator;
    account.receiver = receiver;
```

Recommendations:

Exvul Web3 Security recommends that

Result: Confirmed

Fix Result: fixed

Customer response:

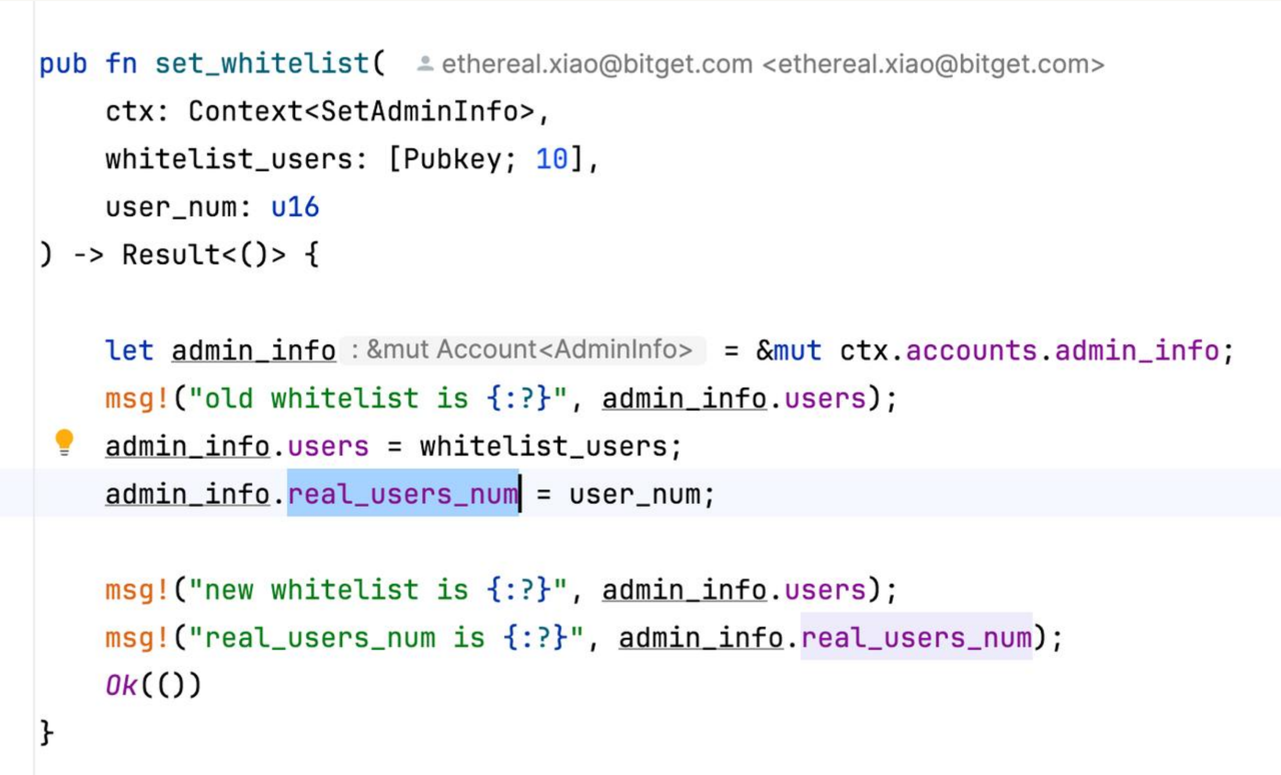
Added authority, operator, receiver, stable_token_receiverother_token_receiver not 0 address

3.6 Allowlist should check users count

ID:	NVE-006	**Location:**	lib.rs
Severity:	Low	**Category:**	Business Issues
Likelihood:	Low	**Impact:**	Low

Description:

Here should check whether the real_users_num is equal to the number of users.



```
pub fn set_whitelist(  ethereal.xiao@bitget.com <ethereal.xiao@bitget.com>
    ctx: Context<SetAdminInfo>,
    whitelist_users: [Pubkey; 10],
    user_num: u16
) -> Result<()> {

    let admin_info : &mut Account<AdminInfo> = &mut ctx.accounts.admin_info;
    msg!("old whitelist is {:?}", admin_info.users);
    admin_info.users = whitelist_users;
    admin_info.real_users_num = user_num;

    msg!("new whitelist is {:?}", admin_info.users);
    msg!("real_users_num is {:?}", admin_info.real_users_num);
    Ok(())
}
```

Recommendations:

Exvul Web3 Security recommends that

Result: Confirmed

Fix Result: fixed

Customer response: added

Fixed version: 89a6cd4ada6c8a6fcd84567a0bbc3c5a7daa36de

4. CONCLUSION

In this audit, we thoroughly analyzed **bitget 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