# VRust

## Security Assessment

O2Lab VRust Team

10/29/2022 21:15:13

# Contents

## Summary

This report has been prepared for O2Lab VRust Team to discover issues and vulnerabilities in the source code of the O2Lab VRust Team project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis and Manual Review techniques. 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 specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough 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 perspective:

- Enhance 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 | O2Lab VRust Team |
| Platform | Ethereum |
| Language | Solana |
| Crate | stable_swap |
| GitHub Location | https://github.com/parasol-aser/vrust |
| sha256 | Unknown |

## Audit Summary

| | |
|---|---|
| Delivery Date | 10/29/2022 |
| Audit Methodology | Static Analysis |
| Key Components | |

## Vulnerability Summary

| Vulnerability Level | Total |
|---|---|
| Critical | 7 |
| Major | 0 |
| Medium | 0 |
| Minor | 0 |
| Informational | 0 |
| Discussion | 0 |

## Findings

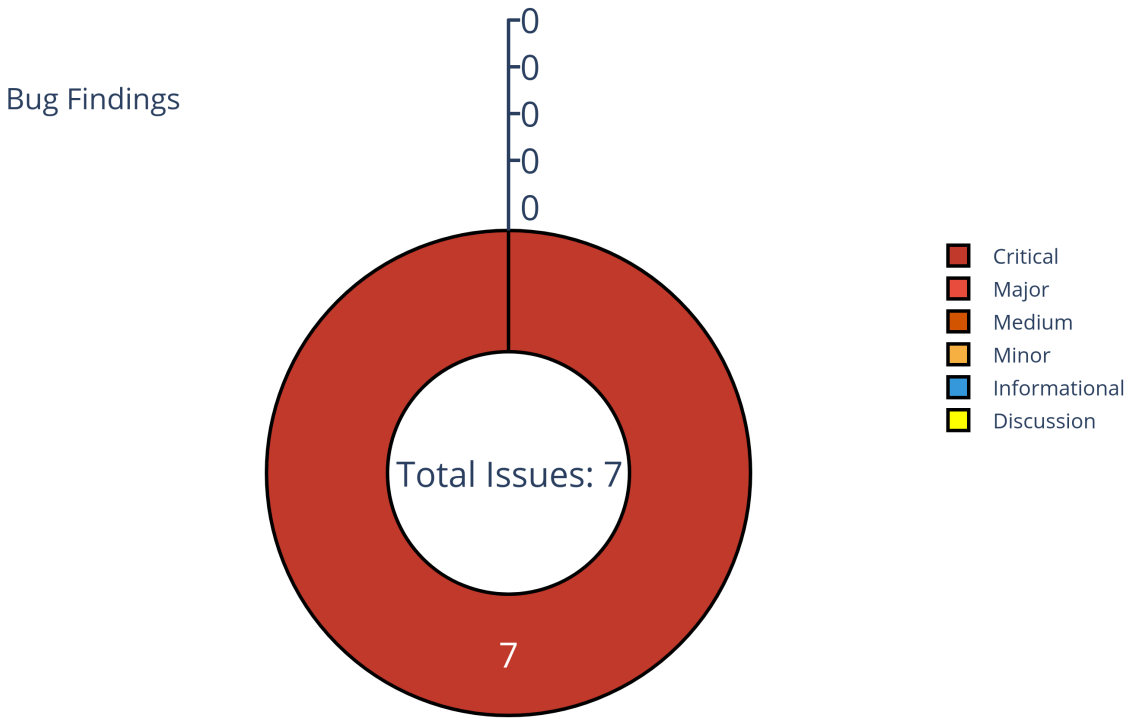


**Figure 1:** Findings

## Finding Statistic

| Category | Count |
| --- | --- |
| MissingKeyCheck | 7 |

| ID | Category | Severity | Status |
| --- | --- | --- | --- |
| 0 | MissingKeyCheck | Critical | UnResolved |
| 1 | MissingKeyCheck | Critical | UnResolved |
| 2 | MissingKeyCheck | Critical | UnResolved |
| 3 | MissingKeyCheck | Critical | UnResolved |
| 4 | MissingKeyCheck | Critical | UnResolved |
| 5 | MissingKeyCheck | Critical | UnResolved |
| 6 | MissingKeyCheck | Critical | UnResolved |

## Issue: 0: MissingKeyCheck

| Category | Severity | Status |
| --- | --- | --- |
| MissingKeyCheck | Critical | UnResolved |

- Location

stable-swap-program/program/src/processor/admin.rs:33:45: 33:72

```
33 swap_info.data.borrow_mut()
34
```

- Code Context

Vulnerability at Line: 33

```
28 ) -> ProgramResult {
29     let account_info_iter = &mut accounts.iter();
30     let swap_info = next_account_info(account_info_iter)?;
31     let admin_info = next_account_info(account_info_iter)?;
32
33     let token_swap = &mut SwapInfo::unpack(&swap_info.data.borrow_mut())?;
34     check_has_admin_signer(&token_swap.admin_key, admin_info)?;
35
36     (match *instruction {
37         AdminInstruction::RampA(RampAData {
38
```

Other Use Case for Variable: swap_info.data.borrow_mut()

```
74     SwapInfo::pack(*token_swap, &mut swap_info.data.borrow_mut())
```

- Call Stack

```
1 fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-
  ↪ 1ecc6299db9ec823/solana-program-1.9.18/src/entrypoint.rs:120:9: 127:10
  ↪ }
2     fn entrypoint::process_instruction(){//
      ↪ stable-swap-program/program/src/entrypoint.rs:11:1: 22:2 }
```

```
3         fn processor::Processor::process(){//
          ↪  stable-swap-program/program/src/processor/mod.rs:26:5: 34:6 }
4             fn processor::admin::process_admin_instruction(){//
               ↪  stable-swap-program/program/src/processor/admin.rs:25:1:
               ↪  75:2 }
5
```

- description:
- link:
- alleviation:

## Issue: 1: MissingKeyCheck

| Category | Severity | Status |
| --- | --- | --- |
| MissingKeyCheck | Critical | UnResolved |

- Location

stable-swap-program/program/src/processor/admin.rs:186:38: 186:76

```
186 new_fee_account_info.data.borrow_mut()
187
```

- Code Context

– Function Definition:

```
179 fn set_fee_account<'a, 'b: 'a, I: Iterator<Item = &'a AccountInfo<'b>>>(
180     token_swap: &mut SwapInfo,
181     account_info_iter: &mut I,
182 ) -> ProgramResult
183
```

Vulnerability at Line: 186

```
181     account_info_iter: &mut I,
182 ) -> ProgramResult {
183     let new_fee_account_info = next_account_info(account_info_iter)?;
184
185     let new_admin_fee_account =
186
            ↪  utils::unpack_token_account(&new_fee_account_info.data.borrow_mut())?;
187     msg!(
188         "Admin: New fee account owner {}",
189         new_admin_fee_account.owner
190     );
191
```

- Call Stack

```
fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.18/src/entrypoint.rs:120:9: 127:10 }
    fn entrypoint::process_instruction(){// stable-swap-program/program/src/entrypoint.rs:11:1: 22:2 }
        fn processor::Processor::process(){// stable-swap-program/program/src/processor/mod.rs:26:5: 34:6 }
            fn processor::admin::process_admin_instruction(){// stable-swap-program/program/src/processor/admin.rs:25:1: 75:2 }
                fn processor::admin::set_fee_account(){// stable-swap-program/program/src/processor/admin.rs:179:1: 210:2 }

```

- description:
- link:
- alleviation:

## Issue: 2: MissingKeyCheck

| Category | Severity | Status |
| --- | --- | --- |
| MissingKeyCheck | Critical | UnResolved |

- Location

stable-swap-program/program/src/processor/swap.rs:708:40: 708:63

```
708 swap_info.data.borrow()
709
```

- Code Context

– Function Definition:

```
681 fn process_withdraw_one(
682     program_id: &Pubkey,
683     pool_token_amount: u64,
684     minimum_token_amount: u64,
685     accounts: &[AccountInfo],
686 ) -> ProgramResult
687
```

Vulnerability at Line: 708

```
703
704     if *base_token_info.key == *quote_token_info.key {
705         return Err(SwapError::InvalidInput.into());
706     }
707
708     let token_swap = SwapInfo::unpack(&swap_info.data.borrow())?;
709     if token_swap.is_paused {
710         return Err(SwapError::IsPaused.into());
711     }
712     check_swap_authority(
713
```

- Call Stack

```
fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.18/src/entrypoint.rs:120:9: 127:10 }
    fn entrypoint::process_instruction(){// stable-swap-program/program/src/entrypoint.rs:11:1: 22:2 }
        fn processor::Processor::process(){// stable-swap-program/program/src/processor/mod.rs:26:5: 34:6 }
            fn processor::swap::process_swap_instruction(){// stable-swap-program/program/src/processor/swap.rs:31:1: 94:2 }
                fn processor::swap::process_withdraw_one(){// stable-swap-program/program/src/processor/swap.rs:681:1: 838:2 }

```

- description:
- link:
- alleviation:

## Issue: 3: MissingKeyCheck

| Category | Severity | Status |
| --- | --- | --- |
| MissingKeyCheck | Critical | UnResolved |

- Location

stable-swap-program/program/src/processor/swap.rs:591:40: 591:63

```
591 swap_info.data.borrow()
592
```

- Code Context

– Function Definition:

```
566 fn process_withdraw(
567     program_id: &Pubkey,
568     pool_token_amount: u64,
569     minimum_token_a_amount: u64,
570     minimum_token_b_amount: u64,
571     accounts: &[AccountInfo],
572 ) -> ProgramResult
573
```

Vulnerability at Line: 591

```
586     let dest_token_b_info = next_account_info(account_info_iter)?;
587     let admin_fee_dest_a_info = next_account_info(account_info_iter)?;
588     let admin_fee_dest_b_info = next_account_info(account_info_iter)?;
589     let token_program_info = next_account_info(account_info_iter)?;
590
591     let token_swap = SwapInfo::unpack(&swap_info.data.borrow())?;
592     check_swap_authority(
593         &token_swap,
594         swap_info.key,
595         program_id,
596
```

- Call Stack

```
fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.18/src/entrypoint.rs:120:9: 127:10 }
    fn entrypoint::process_instruction(){// stable-swap-program/program/src/entrypoint.rs:11:1: 22:2 }
        fn processor::Processor::process(){// stable-swap-program/program/src/processor/mod.rs:26:5: 34:6 }
            fn processor::swap::process_swap_instruction(){// stable-swap-program/program/src/processor/swap.rs:31:1: 94:2 }
                fn processor::swap::process_withdraw(){// stable-swap-program/program/src/processor/swap.rs:566:1: 678:2 }

```

- description:
- link:
- alleviation:

## Issue: 4: MissingKeyCheck

| Category | Severity | Status |
| --- | --- | --- |
| MissingKeyCheck | Critical | UnResolved |

- Location

stable-swap-program/program/src/processor/swap.rs:442:40: 442:63

```
442 swap_info.data.borrow()
443
```

- Code Context

– Function Definition:

```
419 fn process_deposit(
420     program_id: &Pubkey,
421     token_a_amount: u64,
422     token_b_amount: u64,
423     min_mint_amount: u64,
424     accounts: &[AccountInfo],
425 ) -> ProgramResult
426
```

Vulnerability at Line: 442

```
437     let token_b_info = next_account_info(account_info_iter)?;
438     let pool_mint_info = next_account_info(account_info_iter)?;
439     let dest_info = next_account_info(account_info_iter)?;
440     let token_program_info = next_account_info(account_info_iter)?;
441
442     let token_swap = SwapInfo::unpack(&swap_info.data.borrow())?;
443     if token_swap.is_paused {
444         return Err(SwapError::IsPaused.into());
445     }
446     check_swap_authority(
447
```

- Call Stack

```
fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.18/src/entrypoint.rs:120:9: 127:10 }
    fn entrypoint::process_instruction(){// stable-swap-program/program/src/entrypoint.rs:11:1: 22:2 }
        fn processor::Processor::process(){// stable-swap-program/program/src/processor/mod.rs:26:5: 34:6 }
            fn processor::swap::process_swap_instruction(){// stable-swap-program/program/src/processor/swap.rs:31:1: 94:2 }
                fn processor::swap::process_deposit(){// stable-swap-program/program/src/processor/swap.rs:419:1: 525:2 }

```

- description:
- link:
- alleviation:

## Issue: 5: MissingKeyCheck

| Category | Severity | Status |
| --- | --- | --- |
| MissingKeyCheck | Critical | UnResolved |

- Location

stable-swap-program/program/src/processor/swap.rs:309:40: 309:63

```
309 swap_info.data.borrow()
310
```

- Code Context

– Function Definition:

```
284 fn process_swap(
285     program_id: &Pubkey,
286     amount_in: u64,
287     minimum_amount_out: u64,
288     accounts: &[AccountInfo],
289 ) -> ProgramResult
290
```

Vulnerability at Line: 309

```
304
305     if *swap_source_info.key == *swap_destination_info.key {
306         return Err(SwapError::InvalidInput.into());
307     }
308
309     let token_swap = SwapInfo::unpack(&swap_info.data.borrow())?;
310     if token_swap.is_paused {
311         return Err(SwapError::IsPaused.into());
312     }
313
314
```

- Call Stack

```
fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.18/src/entrypoint.rs:120:9: 127:10 }
    fn entrypoint::process_instruction(){// stable-swap-program/program/src/entrypoint.rs:11:1: 22:2 }
        fn processor::Processor::process(){// stable-swap-program/program/src/processor/mod.rs:26:5: 34:6 }
            fn processor::swap::process_swap_instruction(){// stable-swap-program/program/src/processor/swap.rs:31:1: 94:2 }
                fn processor::swap::process_swap(){// stable-swap-program/program/src/processor/swap.rs:284:1: 416:2 }

```

- description:
- link:
- alleviation:

## Issue: 6: MissingKeyCheck

| Category | Severity | Status |
| --- | --- | --- |
| MissingKeyCheck | Critical | UnResolved |

- Location

stable-swap-program/program/src/processor/swap.rs:123:50: 123:73

```
123 swap_info.data.borrow()
124
```

- Code Context

– Function Definition:

```
97  fn process_initialize(
98      program_id: &Pubkey,
99      nonce: u8,
100     amp_factor: u64,
101     fees: Fees,
102     accounts: &[AccountInfo],
103 ) -> ProgramResult
104
```

Vulnerability at Line: 123

```
118     if !(MIN_AMP..=MAX_AMP).contains(&amp_factor) {
119         msg!("Invalid amp factor: {}", amp_factor);
120         return Err(SwapError::InvalidInput.into());
121     }
122
123     let token_swap = SwapInfo::unpack_unchecked(&swap_info.data.borrow())?;
124     if token_swap.is_initialized {
125         return Err(SwapError::AlreadyInUse.into());
126     }
127     let swap_authority = utils::authority_id(program_id, swap_info.key,
        ↪  nonce)?;
128
```

- Call Stack

```
fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.18/src/entrypoint.rs:120:9: 127:10 }
    fn entrypoint::process_instruction(){// stable-swap-program/program/src/entrypoint.rs:11:1: 22:2 }
        fn processor::Processor::process(){// stable-swap-program/program/src/processor/mod.rs:26:5: 34:6 }
            fn processor::swap::process_swap_instruction(){// stable-swap-program/program/src/processor/swap.rs:31:1: 94:2 }
                fn processor::swap::process_initialize(){// stable-swap-program/program/src/processor/swap.rs:97:1: 281:2 }

```

- description:
- link:
- alleviation:

# Appendix

Copied from https://leaderboard.certik.io/projects/aave

## Finding Categories

### Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimal EVM opcodes resulting in a reduction on the total gas cost of a transaction.

### Mathematical Operations

Mathematical Operation findings relate to mishandling of math formulas, such as overflows, incorrect operations etc.

### Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on how block.timestamp works.

### Language Specific

Language Specific findings are issues that would only arise within Solidity, i.e. incorrect usage of private or delete.

### Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to make the codebase more legible and, as a result, easily maintainable.

## Checksum Calculation Method

The “Checksum” field in the “Audit Scope” section is calculated as the SHA-256 (Secure Hash Algorithm 2 with digest size of 256 bits) digest of the content of each file hosted in the listed source repository under the specified commit.

The result is hexadecimal encoded and is the same as the output of the Linux “sha256sum” command against the target file.

## Disclaimer

Copied from https://leaderboard.certik.io/projects/aave

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 you (“Customer” or 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, nor may copies be delivered to any other person other than the Company, without CertiK’s prior written consent in each instance.

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 CertiK 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. CertiK’s position is that each company and individual are responsible for their own due diligence and continuous security. CertiK’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. The assessment services provided by CertiK is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.