VRust

Security Assessment

O2Lab VRust Team

11/04/2022 17:10:34

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	spl_token_2022
GitHub Location	https://github.com/parasol-aser/vrust
sha256	Unknown

Audit Summary

Delivery Date	11/04/2022
Audit Methodology	Static Analysis
Key Components	

Vulnerability Summary

Vulnerability Level	Total
Critical	22
Major	0
Medium	0
Minor	0
Informational	0
Discussion	0

Findings

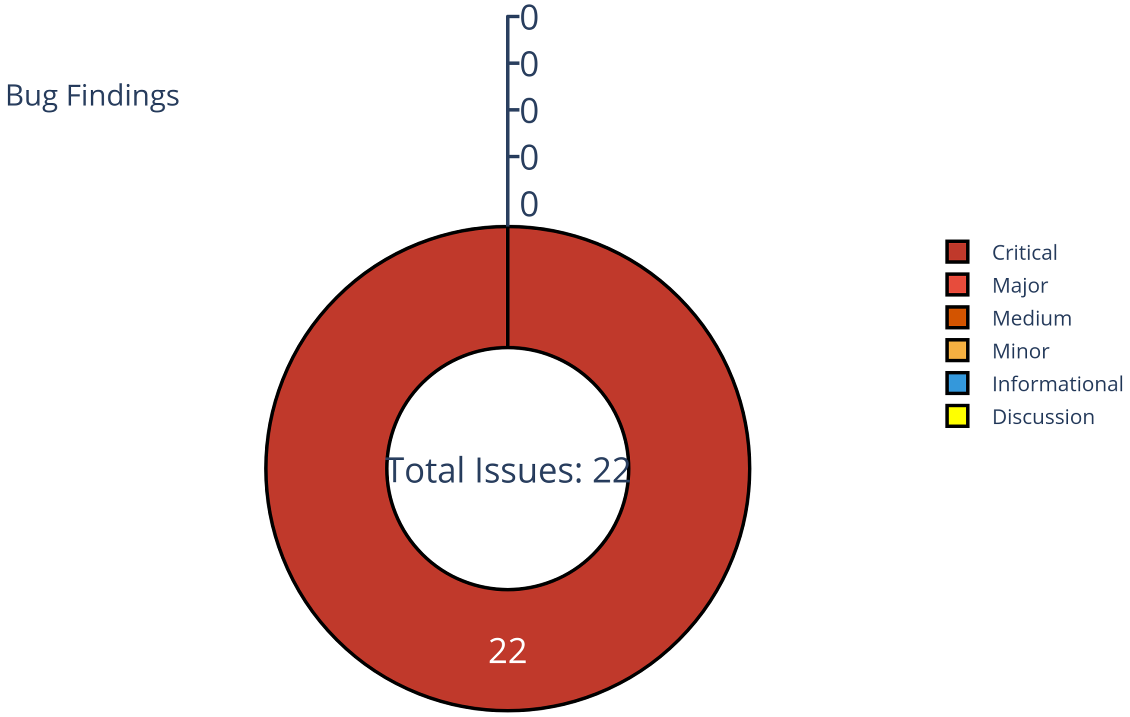

Figure 1: Findings

Finding Statistic

Category	Count
IntegerFlow	1
MissingKeyCheck	21

ID	Category	Severity	Status
0	IntegerFlow	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
7	MissingKeyCheck	Critical	UnResolved
8	MissingKeyCheck	Critical	UnResolved
9	MissingKeyCheck	Critical	UnResolved
10	MissingKeyCheck	Critical	UnResolved
11	MissingKeyCheck	Critical	UnResolved
12	MissingKeyCheck	Critical	UnResolved
13	MissingKeyCheck	Critical	UnResolved
14	MissingKeyCheck	Critical	UnResolved
15	MissingKeyCheck	Critical	UnResolved
16	MissingKeyCheck	Critical	UnResolved
17	MissingKeyCheck	Critical	UnResolved
18	MissingKeyCheck	Critical	UnResolved
19	MissingKeyCheck	Critical	UnResolved
20	MissingKeyCheck	Critical	UnResolved

ID	Category	Severity	Status
21	MissingKeyCheck	Critical	UnResolved

Issue: 0: IntegerFlow

Category	Severity	Status
IntegerFlow	Critical	UnResolved

- Location

/home/yifei/open/vrust/examples2/solana-program-library/token/program/src/lib.rs:35:47: 35:59

```
35 decimals + 1
36
```

- Code Context

Vulnerability at Line: 34

```
31 pub fn amount_to_ui_amount_string(amount: u64, decimals: u8) -> String {
32     let decimals = decimals as usize;
33     if decimals > 0 {
34         // Left-pad zeros to decimals + 1, so we at least have an integer
            ↪  zero
35         let mut s = format!("{:01$}", amount, decimals + 1);
36         // Add the decimal point (Sorry, "," locales!)
37         s.insert(s.len() - decimals, '.');
38         s
39
```

Other Use Case for Variable: decimals + 1

```
35         let mut s = format!("{:01$}", amount, decimals + 1);
```

- Call Stack

```
1 fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-
  ↪   1ecc6299db9ec823/solana-program-1.9.9/src/entrypoint.rs:120:9: 127:10
  ↪   }
2     fn entrypoint::process_instruction(){//
      ↪   token/program-2022/src/entrypoint.rs:12:1: 23:2 }
3         fn processor::Processor::process(){//
          ↪   token/program-2022/src/processor.rs:1112:5: 1261:6 }
```

```
            fn processor::Processor::process_amount_to_ui_amount(){// token/program-2022/src/processor.rs:1034:5: 1047:6 }
                    fn spl_token::amount_to_ui_amount_string_trimmed(){// /home/yifei/open/vrust/examples2/solana-program-library/token/program/src/lib.rs:46:1: 53:2 }
                        fn spl_token::amount_to_ui_amount_string(){// /home/yifei/open/vrust/examples2/solana-program-library/token/program/src/lib.rs:31:1: 42:2 }

```

- description:
- link:
- alleviation:

Issue: 1: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

token/program-2022/src/extension/memo_transfer/processor.rs:60:28: 60:64

```
60 token_account_info.data.borrow_mut()
61
```

- Code Context

– Function Definition:

```
51 fn process_diasble_required_memo_transfers(
52     program_id: &Pubkey,
53     accounts: &[AccountInfo],
54 ) -> ProgramResult
55
```

Vulnerability at Line: 60

```
55     let account_info_iter = &mut accounts.iter();
56     let token_account_info = next_account_info(account_info_iter)?;
57     let owner_info = next_account_info(account_info_iter)?;
58     let owner_info_data_len = owner_info.data_len();
59
60     let mut account_data = token_account_info.data.borrow_mut();
61     let mut account = StateWithExtensionsMut::<Account>::unpack(&mut
        ↪  account_data)?;
62
63     Processor::validate_owner(
64         program_id,
65
```

- Call Stack

```
fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.9/src/entrypoint.rs:120:9: 127:10 }
    fn entrypoint::process_instruction(){// token/program-2022/src/entrypoint.rs:12:1: 23:2 }
        fn processor::Processor::process(){// token/program-2022/src/processor.rs:1112:5: 1261:6 }
            fn extension::memo_transfer::processor::process_instruction(){// token/program-2022/src/extension/memo_transfer/processor.rs:80:1: 98:2 }
                fn extension::memo_transfer::processor::process_diasble_required_memo_tr
                token/program-2022/src/extension/memo_transfer/processor.rs:51:1: 78:2 }

```

- description:
- link:
- alleviation:

Issue: 2: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

token/program-2022/src/extension/memo_transfer/processor.rs:31:28: 31:64

```
31 token_account_info.data.borrow_mut()
32
```

- Code Context

– Function Definition:

```
22 fn process_enable_required_memo_transfers(
23     program_id: &Pubkey,
24     accounts: &[AccountInfo],
25 ) -> ProgramResult
26
```

Vulnerability at Line: 31

```
26     let account_info_iter = &mut accounts.iter();
27     let token_account_info = next_account_info(account_info_iter)?;
28     let owner_info = next_account_info(account_info_iter)?;
29     let owner_info_data_len = owner_info.data_len();
30
31     let mut account_data = token_account_info.data.borrow_mut();
32     let mut account = StateWithExtensionsMut::<Account>::unpack(&mut
        ↪  account_data)?;
33
34     Processor::validate_owner(
35         program_id,
36
```

- Call Stack

```
fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-
↪   1ecc6299db9ec823/solana-program-1.9.9/src/entrypoint.rs:120:9: 127:10
↪   }
    fn entrypoint::process_instruction(){//
    ↪   token/program-2022/src/entrypoint.rs:12:1: 23:2 }
        fn processor::Processor::process(){//
        ↪   token/program-2022/src/processor.rs:1112:5: 1261:6 }
            fn exten-
            ↪   sion::memo_transfer::processor::process_instruction(){//
            ↪   token/program-
            ↪   2022/src/extension/memo_transfer/processor.rs:80:1: 98:2
            ↪   }
                    fn exten-
                    ↪   sion::memo_transfer::processor::process_enable_required_memo_tra
                    ↪   token/program-
                    ↪   2022/src/extension/memo_transfer/processor.rs:22:1:
                    ↪   49:2 }

```

- description:
- link:
- alleviation:

Issue: 3: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

token/program-2022/src/extension/reallocate.rs:34:29: 34:61

```
34 token_account_info.data.borrow()
35
```

- Code Context

Vulnerability at Line: 34

```
29     let authority_info = next_account_info(account_info_iter)?;
30     let authority_info_data_len = authority_info.data_len();
31
32     // check that account is the right type and validate owner
33     let mut current_extension_types = {
34         let token_account = token_account_info.data.borrow();
35         let account = StateWithExtensions::<Account>::unpack(&token_account)?;
36         Processor::validate_owner(
37             program_id,
38             &account.base.owner,
39
```

- Call Stack

```
fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.9/src/entrypoint.rs:120:9: 127:10 }
    fn entrypoint::process_instruction(){// token/program-2022/src/entrypoint.rs:12:1: 23:2 }
        fn processor::Processor::process(){// token/program-2022/src/processor.rs:1112:5: 1261:6 }
            fn extension::reallocate::process_reallocate(){// token/program-2022/src/extension/reallocate.rs:20:1: 87:2 }

```

- description:
- link:
- alleviation:

Issue: 4: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

token/program-2022/src/extension/default_account_state/processor.rs:55:25: 55:60

```
55 mint_account_info.data.borrow_mut()
56
```

- Code Context

– Function Definition:

```
44 fn process_update_default_account_state(
45     program_id: &Pubkey,
46     accounts: &[AccountInfo],
47     state: AccountState,
48 ) -> ProgramResult
49
```

Vulnerability at Line: 55

```
50     let account_info_iter = &mut accounts.iter();
51     let mint_account_info = next_account_info(account_info_iter)?;
52     let freeze_authority_info = next_account_info(account_info_iter)?;
53     let freeze_authority_info_data_len = freeze_authority_info.data_len();
54
55     let mut mint_data = mint_account_info.data.borrow_mut();
56     let mut mint = StateWithExtensionsMut::<Mint>::unpack(&mut mint_data)?;
57
58     let freeze_authority =
59         Op-
         ↪   tion::<Pubkey>::from(mint.base.freeze_authority).ok_or(TokenError::NoAuthori
60
```

- Call Stack

```
fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-
↪  1ecc6299db9ec823/solana-program-1.9.9/src/entrypoint.rs:120:9: 127:10
↪  }
    fn entrypoint::process_instruction(){//
    ↪  token/program-2022/src/entrypoint.rs:12:1: 23:2 }
        fn processor::Processor::process(){//
        ↪  token/program-2022/src/processor.rs:1112:5: 1261:6 }
            fn exten-
            ↪  sion::default_account_state::processor::process_instruction(){//
            ↪  token/program-
            ↪  2022/src/extension/default_account_state/processor.rs:73:1:
            ↪  91:2 }
                    fn exten-
                    ↪  sion::default_account_state::processor::process_update_default_a
                    ↪  token/program-
                    ↪  2022/src/extension/default_account_state/processor.rs:44:1:
                    ↪  71:2 }

```

- description:
- link:
- alleviation:

Issue: 5: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

token/program-2022/src/extension/default_account_state/processor.rs:37:25: 37:60

```
37 mint_account_info.data.borrow_mut()
38
```

- Code Context

– Function Definition:

```
30 fn process_initialize_default_account_state(
31     accounts: &[AccountInfo],
32     state: AccountState,
33 ) -> ProgramResult
34
```

Vulnerability at Line: 37

```
32     state: AccountState,
33 ) -> ProgramResult {
34     check_valid_default_state(state)?;
35     let account_info_iter = &mut accounts.iter();
36     let mint_account_info = next_account_info(account_info_iter)?;
37     let mut mint_data = mint_account_info.data.borrow_mut();
38     let mut mint =
        ↪  StateWithExtensionsMut::<Mint>::unpack_uninitialized(&mut
        ↪  mint_data)?;
39     let extension = mint.init_extension::<DefaultAccountState>()?;
40     extension.state = state.into();
41     Ok(())
42
```

- Call Stack

```
fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-
↪  1ecc6299db9ec823/solana-program-1.9.9/src/entrypoint.rs:120:9: 127:10
↪  }
    fn entrypoint::process_instruction(){//
    ↪  token/program-2022/src/entrypoint.rs:12:1: 23:2 }
        fn processor::Processor::process(){//
        ↪  token/program-2022/src/processor.rs:1112:5: 1261:6 }
            fn exten-
            ↪  sion::default_account_state::processor::process_instruction(){//
            ↪  token/program-
            ↪  2022/src/extension/default_account_state/processor.rs:73:1:
            ↪  91:2 }
                    fn exten-
                    ↪  sion::default_account_state::processor::process_initialize_defau
                    ↪  token/program-
                    ↪  2022/src/extension/default_account_state/processor.rs:30:1:
                    ↪  42:2 }

```

- description:
- link:
- alleviation:

Issue: 6: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

token/program-2022/src/extension/confidential_transfer/processor.rs:1034:25: 1034:60

```
1034 mint_account_info.data.borrow_mut()
1035
```

- Code Context

– Function Definition:

```
1029 fn process_harvest_withheld_tokens_to_mint(accounts: &[AccountInfo]) ->
     ↪  ProgramResult
1030
```

Vulnerability at Line: 1034

```
1029 fn process_harvest_withheld_tokens_to_mint(accounts: &[AccountInfo]) ->
     ↪  ProgramResult {
1030     let account_info_iter = &mut accounts.iter();
1031     let mint_account_info = next_account_info(account_info_iter)?;
1032     let token_account_infos = account_info_iter.as_slice();
1033
1034     let mut mint_data = mint_account_info.data.borrow_mut();
1035     let mut mint = StateWithExtensionsMut::<Mint>::unpack(&mut mint_data)?;
1036     mint.get_extension::<TransferFeeConfig>()?;
1037     let confidential_transfer_mint =
         ↪  mint.get_extension_mut::<ConfidentialTransferMint>()?;
1038
1039
```

- Call Stack

```
fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-
↪  1ecc6299db9ec823/solana-program-1.9.9/src/entrypoint.rs:120:9: 127:10
↪  }
    fn entrypoint::process_instruction(){//
    ↪  token/program-2022/src/entrypoint.rs:12:1: 23:2 }
        fn processor::Processor::process(){//
        ↪  token/program-2022/src/processor.rs:1112:5: 1261:6 }
            fn exten-
            ↪  sion::confidential_transfer::processor::process_instruction(){//
            ↪  token/program-
            ↪  2022/src/extension/confidential_transfer/processor.rs:1058:1:
            ↪  1164:2 }
                    fn exten-
                    ↪  sion::confidential_transfer::processor::process_harvest_withheld
                    ↪  token/program-
                    ↪  2022/src/extension/confidential_transfer/processor.rs:1029:1:
                    ↪  1056:2 }

```

- description:
- link:
- alleviation:

Issue: 7: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

token/program-2022/src/extension/confidential_transfer/processor.rs:910:25: 910:60

```
910 mint_account_info.data.borrow_mut()
911
```

- Code Context

– Function Definition:

```
893 fn process_withdraw_withheld_tokens_from_accounts(
894     program_id: &Pubkey,
895     accounts: &[AccountInfo],
896     num_token_accounts: u8,
897     proof_instruction_offset: i64,
898 ) -> ProgramResult
899
```

Vulnerability at Line: 910

```
905     let account_infos = account_info_iter.as_slice();
906     let num_signers = account_infos
907         .len()
908         .saturating_sub(num_token_accounts as usize);
909
910     let mut mint_data = mint_account_info.data.borrow_mut();
911     let mut mint = StateWithExtensionsMut::<Mint>::unpack(&mut mint_data)?;
912
913     // mint must be extended for fees
914     let transfer_fee_config = mint.get_extension::<TransferFeeConfig>()?;
915
```

- Call Stack

```
fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-
↪   1ecc6299db9ec823/solana-program-1.9.9/src/entrypoint.rs:120:9: 127:10
↪   }
    fn entrypoint::process_instruction(){//
    ↪   token/program-2022/src/entrypoint.rs:12:1: 23:2 }
        fn processor::Processor::process(){//
        ↪   token/program-2022/src/processor.rs:1112:5: 1261:6 }
            fn exten-
            ↪   sion::confidential_transfer::processor::process_instruction(){//
            ↪   token/program-
            ↪   2022/src/extension/confidential_transfer/processor.rs:1058:1:
            ↪   1164:2 }
                    fn exten-
                    ↪   sion::confidential_transfer::processor::process_withdraw_withhel
                    ↪   token/program-
                    ↪   2022/src/extension/confidential_transfer/processor.rs:893:1:
                    ↪   1004:2 }

```

- description:
- link:
- alleviation:

Issue: 8: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

token/program-2022/src/extension/confidential_transfer/processor.rs:818:25: 818:60

```
818 mint_account_info.data.borrow_mut()
819
```

- Code Context

– Function Definition:

```
806 fn process_withdraw_withheld_tokens_from_mint(
807     program_id: &Pubkey,
808     accounts: &[AccountInfo],
809     proof_instruction_offset: i64,
810 ) -> ProgramResult
811
```

Vulnerability at Line: 818

```
813     let dest_account_info = next_account_info(account_info_iter)?;
814     let instructions_sysvar_info = next_account_info(account_info_iter)?;
815     let authority_info = next_account_info(account_info_iter)?;
816     let authority_info_data_len = authority_info.data_len();
817
818     let mut mint_data = mint_account_info.data.borrow_mut();
819     let mut mint = StateWithExtensionsMut::<Mint>::unpack(&mut mint_data)?;
820
821     // mint must be extended for fees
822     {
823
```

- Call Stack

```
fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-
↪   1ecc6299db9ec823/solana-program-1.9.9/src/entrypoint.rs:120:9: 127:10
↪   }
    fn entrypoint::process_instruction(){//
    ↪   token/program-2022/src/entrypoint.rs:12:1: 23:2 }
        fn processor::Processor::process(){//
        ↪   token/program-2022/src/processor.rs:1112:5: 1261:6 }
            fn exten-
            ↪   sion::confidential_transfer::processor::process_instruction(){//
            ↪   token/program-
            ↪   2022/src/extension/confidential_transfer/processor.rs:1058:1:
            ↪   1164:2 }
                    fn exten-
                    ↪   sion::confidential_transfer::processor::process_withdraw_withhel
                    ↪   token/program-
                    ↪   2022/src/extension/confidential_transfer/processor.rs:806:1:
                    ↪   891:2 }

```

- description:
- link:
- alleviation:

Issue: 9: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

token/program-2022/src/extension/transfer_fee/processor.rs:72:25: 72:60

```
72 mint_account_info.data.borrow_mut()
73
```

- Code Context

– Function Definition:

```
61 fn process_set_transfer_fee(
62     program_id: &Pubkey,
63     accounts: &[AccountInfo],
64     transfer_fee_basis_points: u16,
65     maximum_fee: u64,
66 ) -> ProgramResult
67
```

Vulnerability at Line: 72

```
67     let account_info_iter = &mut accounts.iter();
68     let mint_account_info = next_account_info(account_info_iter)?;
69     let authority_info = next_account_info(account_info_iter)?;
70     let authority_info_data_len = authority_info.data_len();
71
72     let mut mint_data = mint_account_info.data.borrow_mut();
73     let mut mint = StateWithExtensionsMut::<Mint>::unpack(&mut mint_data)?;
74     let extension = mint.get_extension_mut::<TransferFeeConfig>()?;
75
76     let transfer_fee_config_authority =
77
```

- Call Stack

```
fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.9/src/entrypoint.rs:120:9: 127:10 }
    fn entrypoint::process_instruction(){// token/program-2022/src/entrypoint.rs:12:1: 23:2 }
        fn processor::Processor::process(){// token/program-2022/src/processor.rs:1112:5: 1261:6 }
            fn extension::transfer_fee::processor::process_instruction(){// token/program-2022/src/extension/transfer_fee/processor.rs:270:1: 318:2 }
                fn extension::transfer_fee::processor::process_set_transfer_fee(){// token/program-2022/src/extension/transfer_fee/processor.rs:61:1: 109:2 }

```

- description:
- link:
- alleviation:

Issue: 10: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

token/program-2022/src/processor.rs:278:39: 278:76

```
278 source_account_info.data.borrow_mut()
279
```

- Code Context

Vulnerability at Line: 278

```
273
274         let dest_account_info = next_account_info(account_info_iter)?;
275         let authority_info = next_account_info(account_info_iter)?;
276         let authority_info_data_len = authority_info.data_len();
277
278         let mut source_account_data =
          ↪   source_account_info.data.borrow_mut();
279         let mut source_account =
280             StateWithExtensionsMut::<Account>::unpack(&mut
              ↪   source_account_data)?;
281         if source_account.base.is_frozen() {
282             return Err(TokenError::AccountFrozen.into());
283
```

- Call Stack

```
1 fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-
  ↪   1ecc6299db9ec823/solana-program-1.9.9/src/entrypoint.rs:120:9: 127:10
  ↪   }
2     fn entrypoint::process_instruction(){//
      ↪   token/program-2022/src/entrypoint.rs:12:1: 23:2 }
3         fn processor::Processor::process(){//
          ↪   token/program-2022/src/processor.rs:1112:5: 1261:6 }
4             fn extension::transfer_fee::processor::process_instruction(){//
              ↪   token/program-
              ↪   2022/src/extension/transfer_fee/processor.rs:270:1: 318:2
              ↪   }
```

```
                    fn processor::Processor::process_transfer(){// token/program-2022/src/processor.rs:257:5: 434:6 }

```

- description:
- link:
- alleviation:

Issue: 11: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

token/program-2022/src/extension/transfer_fee/processor.rs:37:25: 37:60

```
37  mint_account_info.data.borrow_mut()
38
```

- Code Context

– Function Definition:

```
27  fn process_initialize_transfer_fee_config(
28      accounts: &[AccountInfo],
29      transfer_fee_config_authority: COption<Pubkey>,
30      withdraw_withheld_authority: COption<Pubkey>,
31      transfer_fee_basis_points: u16,
32      maximum_fee: u64,
33  ) -> ProgramResult
34
```

Vulnerability at Line: 37

```
32      maximum_fee: u64,
33  ) -> ProgramResult {
34      let account_info_iter = &mut accounts.iter();
35      let mint_account_info = next_account_info(account_info_iter)?;
36
37      let mut mint_data = mint_account_info.data.borrow_mut();
38      let mut mint =
        ↪   StateWithExtensionsMut::<Mint>::unpack_uninitialized(&mut
        ↪   mint_data)?;
39      let extension = mint.init_extension::<TransferFeeConfig>()?;
40      extension.transfer_fee_config_authority =
    ↪   transfer_fee_config_authority.try_into()?;
    extension.withdraw_withheld_authority = withdraw_withheld_authority.try_into()?;

```

- Call Stack

```
fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.9/src/entrypoint.rs:120:9: 127:10 }
    fn entrypoint::process_instruction(){// token/program-2022/src/entrypoint.rs:12:1: 23:2 }
        fn processor::Processor::process(){// token/program-2022/src/processor.rs:1112:5: 1261:6 }
            fn extension::transfer_fee::processor::process_instruction(){// token/program-2022/src/extension/transfer_fee/processor.rs:270:1: 318:2 }
                    fn extension::transfer_fee::processor::process_initialize_transfer_fee_c
                    token/program-2022/src/extension/transfer_fee/processor.rs:27:1: 59:2 }

```

- description:
- link:
- alleviation:

Issue: 12: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

token/program-2022/src/processor.rs:996:29: 996:64

```
996  mint_account_info.data.borrow_mut()
997
```

- Code Context

Vulnerability at Line: 996

```
991          close_authority: COption<Pubkey>,
992      ) -> ProgramResult {
993          let account_info_iter = &mut accounts.iter();
994          let mint_account_info = next_account_info(account_info_iter)?;
995
996          let mut mint_data = mint_account_info.data.borrow_mut();
997          let mut mint =
             ↪   StateWithExtensionsMut::<Mint>::unpack_uninitialized(&mut
             ↪   mint_data)?;
998          let extension = mint.init_extension::<MintCloseAuthority>()?;
999          extension.close_authority = close_authority.try_into()?;
1000
1001
```

- Call Stack

```
fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-
↪   1ecc6299db9ec823/solana-program-1.9.9/src/entrypoint.rs:120:9: 127:10
↪   }
    fn entrypoint::process_instruction(){//
    ↪   token/program-2022/src/entrypoint.rs:12:1: 23:2 }
        fn processor::Processor::process(){//
        ↪   token/program-2022/src/processor.rs:1112:5: 1261:6 }
```

```
            fn processor::Processor::process_initialize_mint_close_authority(){// token/program-2022/src/processor.rs:989:5: 1002:6 }

```

- description:
- link:
- alleviation:

Issue: 13: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

token/program-2022/src/processor.rs:1027:39: 1027:75

```
token_account_info.data.borrow_mut()
```

- Code Context

Vulnerability at Line: 1027

```
pub fn process_initialize_immutable_owner(accounts: &[AccountInfo]) -> ProgramResult {
        let account_info_iter = &mut accounts.iter();
        let token_account_info = next_account_info(account_info_iter)?;
        let token_account_data = &mut token_account_info.data.borrow_mut();
        let mut token_account =
            StateWithExtensionsMut::<Account>::unpack_uninitialized(token_account_data)?;
        token_account.init_extension::<ImmutableOwner>().map(|_| ())
    }
```

- Call Stack

```
fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.9/src/entrypoint.rs:120:9: 127:10 }
    fn entrypoint::process_instruction(){// token/program-2022/src/entrypoint.rs:12:1: 23:2 }
        fn processor::Processor::process(){// token/program-2022/src/processor.rs:1112:5: 1261:6 }
            fn processor::Processor::process_initialize_immutable_owner(){// token/program-2022/src/processor.rs:1024:5: 1031:6 }
```

- description:
- link:
- alleviation:

Issue: 14: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

token/program-2022/src/processor.rs:1305:25: 1305:56

```
1305 mint_account_info.data.borrow()
1306
```

- Code Context

– Function Definition:

```
1302 fn get_required_account_extensions(
1303         mint_account_info: &AccountInfo,
1304     ) -> Result<Vec<ExtensionType>, ProgramError>
1305
```

Vulnerability at Line: 1305

```
1302 fn get_required_account_extensions(
1303         mint_account_info: &AccountInfo,
1304     ) -> Result<Vec<ExtensionType>, ProgramError> {
1305         let mint_data = mint_account_info.data.borrow();
1306         let state = StateWithExtensions::<Mint>::unpack(&mint_data)
1307             .map_err(|_|
       ↪  Into::<ProgramError>::into(TokenError::InvalidMint))?;
1308
               ↪   Self::get_required_account_extensions_from_unpacked_mint(mint_account_info.c
               ↪   &state)
1309     }
1310
```

- Call Stack

```
fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.9/src/entrypoint.rs:120:9: 127:10 }
    fn entrypoint::process_instruction(){// token/program-2022/src/entrypoint.rs:12:1: 23:2 }
        fn processor::Processor::process(){// token/program-2022/src/processor.rs:1112:5: 1261:6 }
            fn processor::Processor::process_get_account_data_size(){// token/program-2022/src/processor.rs:1005:5: 1021:6 }
                    fn processor::Processor::get_required_account_extensions(){// token/program-2022/src/processor.rs:1302:5: 1309:6 }

```

- description:
- link:
- alleviation:

Issue: 15: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

token/program-2022/src/processor.rs:143:25: 143:48

```
143 mint_info.data.borrow()
144
```

- Code Context

– Function Definition:

```
113 fn _process_initialize_account(
114         accounts: &[AccountInfo],
115         owner: Option<&Pubkey>,
116         rent_sysvar_account: bool,
117     ) -> ProgramResult
118
```

Vulnerability at Line: 143

```
138         if !rent.is_exempt(new_account_info.lamports(),
             ↪  new_account_info_data_len) {
139             return Err(TokenError::NotRentExempt.into());
140         }
141
142         // get_required_account_extensions checks mint validity
143         let mint_data = mint_info.data.borrow();
144         let mint = StateWithExtensions::<Mint>::unpack(&mint_data)
145             .map_err(|_|
 ↪  Into::<ProgramError>::into(TokenError::InvalidMint))?;
146         let required_extensions =
147
                 ↪  Self::get_required_account_extensions_from_unpacked_mint(mint_info.owner
                 ↪  &mint)?;
148
```

- Call Stack

```
fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.9/src/entrypoint.rs:120:9: 127:10 }
    fn entrypoint::process_instruction(){// token/program-2022/src/entrypoint.rs:12:1: 23:2 }
        fn processor::Processor::process(){// token/program-2022/src/processor.rs:1112:5: 1261:6 }
            fn processor::Processor::process_initialize_account3(){// token/program-2022/src/processor.rs:200:5: 202:6 }
                    fn processor::Processor::_process_initialize_account(){// token/program-2022/src/processor.rs:113:5: 187:6 }

```

- description:
- link:
- alleviation:

Issue: 16: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

token/program-2022/src/processor.rs:760:39: 760:76

```
source_account_info.data.borrow_mut()

```

- Code Context

Vulnerability at Line: 760

```
        let source_account_info = next_account_info(account_info_iter)?;
        let mint_info = next_account_info(account_info_iter)?;
        let authority_info = next_account_info(account_info_iter)?;
        let authority_info_data_len = authority_info.data_len();

        let mut source_account_data =
         ↪   source_account_info.data.borrow_mut();
        let mut source_account =
            StateWithExtensionsMut::<Account>::unpack(&mut
             ↪   source_account_data)?;
        let mut mint_data = mint_info.data.borrow_mut();
        let mut mint = StateWithExtensionsMut::<Mint>::unpack(&mut
         ↪   mint_data)?;

```

- Call Stack

```
fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-
 ↪   1ecc6299db9ec823/solana-program-1.9.9/src/entrypoint.rs:120:9: 127:10
 ↪   }
    fn entrypoint::process_instruction(){//
     ↪   token/program-2022/src/entrypoint.rs:12:1: 23:2 }
        fn processor::Processor::process(){//
         ↪   token/program-2022/src/processor.rs:1112:5: 1261:6 }
```

```
            fn processor::Processor::process_burn(){// token/program-2022/src/processor.rs:747:5: 837:6 }

```

- description:
- link:
- alleviation:

Issue: 17: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

token/program-2022/src/processor.rs:690:37: 690:72

```
690 dest_account_info.data.borrow_mut()
691
```

- Code Context

Vulnerability at Line: 690

```
685         let mint_info = next_account_info(account_info_iter)?;
686         let dest_account_info = next_account_info(account_info_iter)?;
687         let owner_info = next_account_info(account_info_iter)?;
688         let owner_info_data_len = owner_info.data_len();
689
690         let mut dest_account_data = dest_account_info.data.borrow_mut();
691         let mut dest_account =
         ↪   StateWithExtensionsMut::<Account>::unpack(&mut
         ↪   dest_account_data)?;
692         if dest_account.base.is_frozen() {
693             return Err(TokenError::AccountFrozen.into());
694         }
695
```

- Call Stack

```
1 fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-
  ↪   1ecc6299db9ec823/solana-program-1.9.9/src/entrypoint.rs:120:9: 127:10
  ↪   }
2     fn entrypoint::process_instruction(){//
      ↪   token/program-2022/src/entrypoint.rs:12:1: 23:2 }
3         fn processor::Processor::process(){//
          ↪   token/program-2022/src/processor.rs:1112:5: 1261:6 }
          fn processor::Processor::process_mint_to(){// token/program-2022/src/processor.rs:678:5: 744:6 }

```

- description:
- link:
- alleviation:

Issue: 18: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

token/program-2022/src/processor.rs:456:39: 456:76

```
456 source_account_info.data.borrow_mut()
457
```

- Code Context

Vulnerability at Line: 456

```
451         };
452         let delegate_info = next_account_info(account_info_iter)?;
453         let owner_info = next_account_info(account_info_iter)?;
454         let owner_info_data_len = owner_info.data_len();
455
456         let mut source_account_data =
             ↪  source_account_info.data.borrow_mut();
457         let mut source_account =
458             StateWithExtensionsMut::<Account>::unpack(&mut
                 ↪  source_account_data)?;
459
460         if source_account.base.is_frozen() {
461
```

- Call Stack

```
1 fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-
  ↪  1ecc6299db9ec823/solana-program-1.9.9/src/entrypoint.rs:120:9: 127:10
  ↪  }
2     fn entrypoint::process_instruction(){//
      ↪  token/program-2022/src/entrypoint.rs:12:1: 23:2 }
3         fn processor::Processor::process(){//
          ↪  token/program-2022/src/processor.rs:1112:5: 1261:6 }
```

```
            fn processor::Processor::process_approve(){// token/program-2022/src/processor.rs:437:5: 489:6 }

```

- description:
- link:
- alleviation:

Issue: 19: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

token/program-2022/src/processor.rs:923:39: 923:76

```
923 source_account_info.data.borrow_mut()
924
```

- Code Context

Vulnerability at Line: 923

```
918         let source_account_info = next_account_info(account_info_iter)?;
919         let mint_info = next_account_info(account_info_iter)?;
920         let authority_info = next_account_info(account_info_iter)?;
921         let authority_info_data_len = authority_info.data_len();
922
923         let mut source_account_data =
             ↪   source_account_info.data.borrow_mut();
924         let mut source_account =
925             StateWithExtensionsMut::<Account>::unpack(&mut
                 ↪   source_account_data)?;
926         if freeze && source_account.base.is_frozen() || !freeze &&
             ↪   !source_account.base.is_frozen()
927         {
928
```

- Call Stack

```
fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-
↪   1ecc6299db9ec823/solana-program-1.9.9/src/entrypoint.rs:120:9: 127:10
↪   }
    fn entrypoint::process_instruction(){//
    ↪   token/program-2022/src/entrypoint.rs:12:1: 23:2 }
        fn processor::Processor::process(){//
        ↪   token/program-2022/src/processor.rs:1112:5: 1261:6 }
```

```
            fn processor::Processor::process_toggle_freeze_account(){// token/program-2022/src/processor.rs:912:5: 959:6 }

```

- description:
- link:
- alleviation:

Issue: 20: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

token/program-2022/src/processor.rs:537:32: 537:62

```
account_info.data.borrow_mut()

```

- Code Context

Vulnerability at Line: 537

```
        let account_info_iter = &mut accounts.iter();
        let account_info = next_account_info(account_info_iter)?;
        let authority_info = next_account_info(account_info_iter)?;
        let authority_info_data_len = authority_info.data_len();

        let mut account_data = account_info.data.borrow_mut();
        if let Ok(mut account) =
        ↪   StateWithExtensionsMut::<Account>::unpack(&mut account_data) {
            if account.base.is_frozen() {
                return Err(TokenError::AccountFrozen.into());
            }

```

- Call Stack

```
fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-
↪   1ecc6299db9ec823/solana-program-1.9.9/src/entrypoint.rs:120:9: 127:10
↪   }
    fn entrypoint::process_instruction(){//
    ↪   token/program-2022/src/entrypoint.rs:12:1: 23:2 }
        fn processor::Processor::process(){//
        ↪   token/program-2022/src/processor.rs:1112:5: 1261:6 }
            fn processor::Processor::process_set_authority(){//
            ↪   token/program-2022/src/processor.rs:526:5: 675:6 }

```

- description:
- link:
- alleviation:

Issue: 21: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

token/program-2022/src/processor.rs:498:39: 498:76

```
498  source_account_info.data.borrow_mut()
499
```

- Code Context

Vulnerability at Line: 498

```
493          let account_info_iter = &mut accounts.iter();
494          let source_account_info = next_account_info(account_info_iter)?;
495          let authority_info = next_account_info(account_info_iter)?;
496          let authority_info_data_len = authority_info.data_len();
497
498          let mut source_account_data =
              ↪  source_account_info.data.borrow_mut();
499          let mut source_account =
500              StateWithExtensionsMut::<Account>::unpack(&mut
                  ↪  source_account_data)?;
501          if source_account.base.is_frozen() {
502              return Err(TokenError::AccountFrozen.into());
503
```

- Call Stack

```
1  fn entrypoint::entrypoint(){// /home/yifei/.cargo/registry/src/github.com-
   ↪  1ecc6299db9ec823/solana-program-1.9.9/src/entrypoint.rs:120:9: 127:10
   ↪  }
2      fn entrypoint::process_instruction(){//
       ↪  token/program-2022/src/entrypoint.rs:12:1: 23:2 }
3          fn processor::Processor::process(){//
           ↪  token/program-2022/src/processor.rs:1112:5: 1261:6 }
```

```
            fn processor::Processor::process_revoke(){// token/program-2022/src/processor.rs:492:5: 523:6 }

```

- 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.