VRust

Security Assessment

O2Lab VRust Team

11/04/2022 17:27:41

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_governance
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	24
Major	0
Medium	0
Minor	0
Informational	0
Discussion	0

Findings

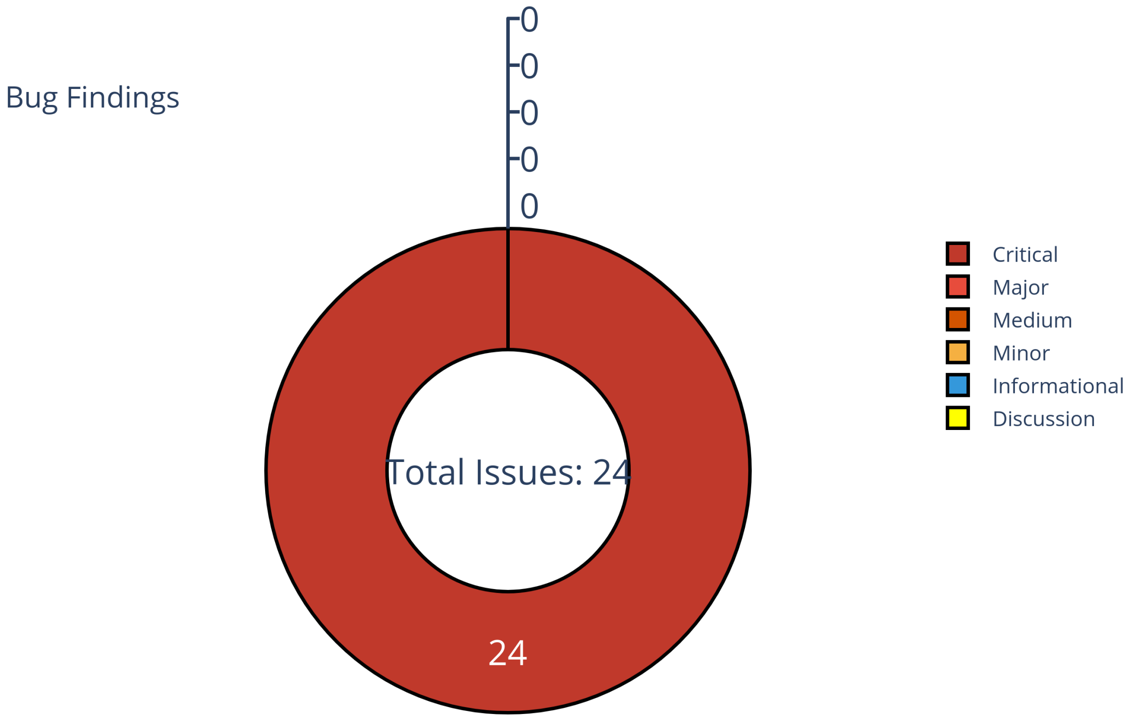

Figure 1: Findings

Finding Statistic

Category	Count
MissingKeyCheck	11
TypeConfusion	13

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
7	MissingKeyCheck	Critical	UnResolved
8	MissingKeyCheck	Critical	UnResolved
9	MissingKeyCheck	Critical	UnResolved
10	MissingKeyCheck	Critical	UnResolved
11	TypeConfusion	Critical	GitHub Link to be added.
12	TypeConfusion	Critical	GitHub Link to be added.
13	TypeConfusion	Critical	GitHub Link to be added.
14	TypeConfusion	Critical	GitHub Link to be added.
15	TypeConfusion	Critical	GitHub Link to be added.
16	TypeConfusion	Critical	GitHub Link to be added.
17	TypeConfusion	Critical	GitHub Link to be added.
18	TypeConfusion	Critical	GitHub Link to be added.
19	TypeConfusion	Critical	GitHub Link to be added.
20	TypeConfusion	Critical	GitHub Link to be added.

ID	Category	Severity	Status
21	TypeConfusion	Critical	GitHub Link to be added.
22	TypeConfusion	Critical	GitHub Link to be added.
23	TypeConfusion	Critical	GitHub Link to be added.

Issue: 0: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

/home/yifei/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.9.9/src/account_info.rs:66:11: 66:33

```
self.lamports.borrow()

```

- Code Context

Vulnerability at Line: 66

```
pub fn lamports(&self) -> u64 {
        **self.lamports.borrow()
    }

```

- Call Stack

```
fn entrypoint::process_instruction(){//
↪   governance/program/src/entrypoint.rs:11:1: 22:2 }
    fn processor::process_instruction(){//
    ↪   governance/program/src/processor/mod.rs:65:1: 217:2 }
        fn proces-
        ↪   sor::process_create_native_treasury::process_create_native_treasury(){//
        ↪   gover-
        ↪   nance/program/src/processor/process_create_native_treasury.rs:19:1:
        ↪   48:2 }
            fn
            ↪   spl_governance_tools::account::create_and_serialize_account_with_owner_s
            ↪   /home/yifei/open/vrust/examples2/solana-program-
            ↪   library/governance/tools/src/account.rs:108:1: 203:2
            ↪   }
                    fn
                    ↪   solana_program::account_info::AccountInfo::<'a>::lamports(){//
                    ↪   /home/yifei/.cargo/registry/src/github.com-
                    ↪   1ecc6299db9ec823/solana-program-
                    ↪   1.9.9/src/account_info.rs:65:5: 67:6
                    ↪   }
```

- description:
- link:
- alleviation:

Issue: 1: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

/home/yifei/open/vrust/examples2/solana-program-library/governance/tools/src/account.rs:199:38:199:68

```
199 account_info.data.borrow_mut()
200
```

- Code Context

Vulnerability at Line: 199

```
194         account_info
195             .data
196             .borrow_mut()
197             .copy_from_slice(&serialized_data);
198     } else if account_size > 0 {
199         account_data.serialize(&mut *account_info.data.borrow_mut())?;
200     }
201
202     Ok(())
203 }
204
```

- Call Stack

```
fn entrypoint::process_instruction(){// governance/program/src/entrypoint.rs:11:1: 22:2 }
    fn processor::process_instruction(){// governance/program/src/processor/mod.rs:65:1: 217:2 }
        fn processor::process_create_native_treasury::process_create_native_treasury(){// governance/program/src/processor/process_create_native_treasury.rs:19:1: 48:2 }
```

```
fn
↪  spl_governance_tools::account::create_and_serialize_account_with_owner_s
↪  /home/yifei/open/vrust/examples2/solana-program-
↪  library/governance/tools/src/account.rs:108:1: 203:2
↪  }

```

- description:
- link:
- alleviation:

Issue: 2: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

governance/program/src/state/realm.rs:298:73: 298:97

```
298 realm_info.data.borrow()
299
```

- Code Context

Vulnerability at Line: 298

```
294 pub fn get_realm_data(
295     program_id: &Pubkey,
296     realm_info: &AccountInfo,
297 ) -> Result<RealmV2, ProgramError> {
298     let account_type: GovernanceAccountType = try_from_slice_unchecked(&realm_info.data.borrow())?;
299
300     // If the account is V1 version then translate to V2
301     if account_type == GovernanceAccountType::RealmV1 {
302         let realm_data_v1 = get_account_data::<RealmV1>(program_id, realm_info)?;
303
```

- Call Stack

```
fn entrypoint::process_instruction(){// governance/program/src/entrypoint.rs:11:1: 22:2 }
    fn processor::process_instruction(){// governance/program/src/processor/mod.rs:65:1: 217:2 }
        fn processor::process_create_token_owner_record::process_create_token_owner_record(){// governance/program/src/processor/process_create_token_owner_record.rs:22:1: 70:2 }
            fn state::realm::get_realm_data(){// governance/program/src/state/realm.rs:294:1: 318:2 }
```

```

```

- description:
- link:
- alleviation:

Issue: 3: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

governance/program/src/state/proposal.rs:848:35: 848:62

```
848 proposal_info.data.borrow()
849
```

- Code Context

Vulnerability at Line: 848

```
843 pub fn get_proposal_data(
844     program_id: &Pubkey,
845     proposal_info: &AccountInfo,
846 ) -> Result<ProposalV2, ProgramError> {
847     let account_type: GovernanceAccountType =
848         try_from_slice_unchecked(&proposal_info.data.borrow())?;
849
850     // If the account is V1 version then translate to V2
851     if account_type == GovernanceAccountType::ProposalV1 {
852         let proposal_data_v1 = get_account_data::<ProposalV1>(program_id,
        ↪   proposal_info)?;
853
```

- Call Stack

```
fn entrypoint::process_instruction(){//
↪  governance/program/src/entrypoint.rs:11:1: 22:2 }
    fn processor::process_instruction(){//
    ↪  governance/program/src/processor/mod.rs:65:1: 217:2 }
        fn proces-
        ↪  sor::process_flag_transaction_error::process_flag_transaction_error(){//
        ↪  gover-
        ↪  nance/program/src/processor/process_flag_transaction_error.rs:19:1:
        ↪  65:2 }
            fn state::proposal::get_proposal_data(){//
            ↪  governance/program/src/state/proposal.rs:843:1: 905:2 }
```

- description:
- link:
- alleviation:

Issue: 4: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

governance/program/src/state/proposal_transaction.rs:213:35: 213:74

```
213 proposal_transaction_info.data.borrow()
214
```

- Code Context

Vulnerability at Line: 213

```
208 pub fn get_proposal_transaction_data(
209     program_id: &Pubkey,
210     proposal_transaction_info: &AccountInfo,
211 ) -> Result<ProposalTransactionV2, ProgramError> {
212     let account_type: GovernanceAccountType =
213
     ↪  try_from_slice_unchecked(&proposal_transaction_info.data.borrow())?;
214
215     // If the account is V1 version then translate to V2
216     if account_type == GovernanceAccountType::ProposalInstructionV1 {
217         let proposal_transaction_data_v1 =
218
```

- Call Stack

```
fn entrypoint::process_instruction(){//
↪  governance/program/src/entrypoint.rs:11:1: 22:2 }
    fn processor::process_instruction(){//
    ↪  governance/program/src/processor/mod.rs:65:1: 217:2 }
        fn proces-
        ↪  sor::process_flag_transaction_error::process_flag_transaction_error(){//
        ↪  gover-
        ↪  nance/program/src/processor/process_flag_transaction_error.rs:19:1:
        ↪  65:2 }
            fn
            ↪  state::proposal_transaction::get_proposal_transaction_data_for_proposal(
            ↪  governance/program/src/state/proposal_transaction.rs:237:1:
            ↪  250:2 }
```

```
                    fn state::proposal_transaction::get_proposal_transaction_data(){// governance/program/src/state/proposal_transaction.rs:208:1: 234:2 }

```

- description:
- link:
- alleviation:

Issue: 5: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

governance/program/src/processor/process_create_token_governance.rs:95:51: 95:84

```
95  governed_token_info.data.borrow()
96
```

- Code Context

Vulnerability at Line: 95

```
90              AuthorityType::AccountOwner,
91              spl_token_info,
92          )?;
93
94          // If the token account has close_authority then transfer it as well
95          let token_account_data = Account::unpack(&governed_token_info.data.borrow())?;
96          // Note: The code assumes owner==close_authority
97          //       If this is not the case then the caller should set close_authority accordingly before making the transfer
98          if token_account_data.close_authority.is_some() {
99              set_spl_token_account_authority(
100
```

- Call Stack

```
fn entrypoint::process_instruction(){// governance/program/src/entrypoint.rs:11:1: 22:2 }
    fn processor::process_instruction(){// governance/program/src/processor/mod.rs:65:1: 217:2 }
        fn processor::process_create_token_governance::process_create_token_governance(){// governance/program/src/processor/process_create_token_governance.rs:27:1: 112:2 }
```

- description:
- link:
- alleviation:

Issue: 6: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

governance/program/src/processor/process_create_mint_governance.rs:97:39: 97:71

```
governed_mint_info.data.borrow()

```

- Code Context

Vulnerability at Line: 97

```
            AuthorityType::MintTokens,
            spl_token_info,
        )?;

        // If the mint has freeze_authority then transfer it as well
        let mint_data = Mint::unpack(&governed_mint_info.data.borrow())?;
        // Note: The code assumes mint_authority==freeze_authority
        //       If this is not the case then the caller should set freeze_authority accordingly before making the transfer
        if mint_data.freeze_authority.is_some() {
            set_spl_token_account_authority(

```

- Call Stack

```
fn entrypoint::process_instruction(){// governance/program/src/entrypoint.rs:11:1: 22:2 }
    fn processor::process_instruction(){// governance/program/src/processor/mod.rs:65:1: 217:2 }
        fn processor::process_create_mint_governance::process_create_mint_governance(){// governance/program/src/processor/process_create_mint_governance.rs:29:1: 117:2 }

```

- description:
- link:
- alleviation:

Issue: 7: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

governance/program/src/state/vote_record.rs:149:35: 149:65

```
149 vote_record_info.data.borrow()
150
```

- Code Context

Vulnerability at Line: 149

```
144 pub fn get_vote_record_data(
145     program_id: &Pubkey,
146     vote_record_info: &AccountInfo,
147 ) -> Result<VoteRecordV2, ProgramError> {
148     let account_type: GovernanceAccountType =
149         try_from_slice_unchecked(&vote_record_info.data.borrow())?;
150
151     // If the account is V1 version then translate to V2
152     if account_type == GovernanceAccountType::VoteRecordV1 {
153         let vote_record_data_v1 =
        ↪   get_account_data::<VoteRecordV1>(program_id,
        ↪   vote_record_info)?;
154
```

- Call Stack

```
fn entrypoint::process_instruction(){//
↪   governance/program/src/entrypoint.rs:11:1: 22:2 }
    fn processor::process_instruction(){//
    ↪   governance/program/src/processor/mod.rs:65:1: 217:2 }
        fn processor::process_relinquish_vote::process_relinquish_vote(){//
        ↪   gover-
        ↪   nance/program/src/processor/process_relinquish_vote.rs:24:1:
        ↪   119:2 }
            fn
            ↪   state::vote_record::get_vote_record_data_for_proposal_and_token_owner(){
            ↪   governance/program/src/state/vote_record.rs:181:1: 198:2 }
```

```
                    fn state::vote_record::get_vote_record_data(){// governance/program/src/state/vote_record.rs:144:1: 178:2 }

```

- description:
- link:
- alleviation:

Issue: 8: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

governance/program/src/state/signatory_record.rs:128:35: 128:70

```
128 signatory_record_info.data.borrow()
129
```

- Code Context

Vulnerability at Line: 128

```
123 pub fn get_signatory_record_data(
124     program_id: &Pubkey,
125     signatory_record_info: &AccountInfo,
126 ) -> Result<SignatoryRecordV2, ProgramError> {
127     let account_type: GovernanceAccountType =
128         try_from_slice_unchecked(&signatory_record_info.data.borrow())?;
129
130     // If the account is V1 version then translate to V2
131     if account_type == GovernanceAccountType::SignatoryRecordV1 {
132         let signatory_record_data_v1 =
133
```

- Call Stack

```
fn entrypoint::process_instruction(){//
↪  governance/program/src/entrypoint.rs:11:1: 22:2 }
    fn processor::process_instruction(){//
    ↪  governance/program/src/processor/mod.rs:65:1: 217:2 }
        fn proces-
        ↪  sor::process_sign_off_proposal::process_sign_off_proposal(){//
        ↪  gover-
        ↪  nance/program/src/processor/process_sign_off_proposal.rs:19:1:
        ↪  99:2 }
            fn
            ↪  state::signatory_record::get_signatory_record_data_for_seeds(){//
            ↪  governance/program/src/state/signatory_record.rs:151:1:
            ↪  167:2 }
```

```
fn state::signatory_record::get_signatory_record_data(){// governance/program/src/state/signatory_record.rs:123:1: 148:2 }

```

- description:
- link:
- alleviation:

Issue: 9: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

governance/program/src/processor/process_sign_off_proposal.rs:67:47: 67:86

```
67 signatory_record_info.data.borrow_mut()
68
```

- Code Context

Vulnerability at Line: 67

```
62         )?;
63
64         signatory_record_data.assert_can_sign_off(signatory_info)?;
65
66         signatory_record_data.signed_off = true;
67         signatory_record_data.serialize(&mut *signatory_record_info.data.borrow_mut())?;
68
69         if proposal_data.signatories_signed_off_count == 0 {
70             proposal_data.signing_off_at = Some(clock.unix_timestamp);
71             proposal_data.state = ProposalState::SigningOff;
72
```

- Call Stack

```
fn entrypoint::process_instruction(){// governance/program/src/entrypoint.rs:11:1: 22:2 }
    fn processor::process_instruction(){// governance/program/src/processor/mod.rs:65:1: 217:2 }
        fn processor::process_sign_off_proposal::process_sign_off_proposal(){// governance/program/src/processor/process_sign_off_proposal.rs:19:1: 99:2 }

```

- description:
- link:
- alleviation:

Issue: 10: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

governance/program/src/processor/process_withdraw_governing_tokens.rs:73:45: 73:86

```
token_owner_record_info.data.borrow_mut()

```

- Code Context

Vulnerability at Line: 73

```
        token_owner_record_data.governing_token_deposit_amount,
        spl_token_info,
    )?;

    token_owner_record_data.governing_token_deposit_amount = 0;
    token_owner_record_data.serialize(&mut *token_owner_record_info.data.borrow_mut())?;

    Ok(())
}

```

- Call Stack

```
fn entrypoint::process_instruction(){// governance/program/src/entrypoint.rs:11:1: 22:2 }
    fn processor::process_instruction(){// governance/program/src/processor/mod.rs:65:1: 217:2 }
        fn processor::process_withdraw_governing_tokens::process_withdraw_governing_tokens(){ governance/program/src/processor/process_withdraw_governing_tokens.rs:21:1: 76:2 }

```

- description:
- link:
- alleviation:

Issue: 11: TypeConfusion

Category	Severity	Status
TypeConfusion	Critical	GitHub Link to be added.

- Location

governance/program/src/instruction.rs:32:69: 32:80

```
BorshSchema
governance/program/src/state/enums.rs:215:69: 215:80
    BorshSchema
governance/program/src/state/enums.rs:215:69: 215:80
    BorshSchema
governance/program/src/state/legacy.rs:322:69: 322:80
    BorshSchema
governance/program/src/state/legacy.rs:322:69: 322:80
    BorshSchema
governance/program/src/state/governance.rs:25:1: 49:2
    pub struct GovernanceConfig {
    /// The type of the vote threshold used for voting
    /// Note: In the current version only YesVote threshold is supported
    pub vote_threshold_percentage: VoteThresholdPercentage,

    /// Minimum community weight a governance token owner must possess to be able to create a proposal
    pub min_community_weight_to_create_proposal: u64,

    /// Minimum waiting time in seconds for a transaction to be executed after proposal is voted on
    pub min_transaction_hold_up_time: u32,

    /// Time limit in seconds for proposal to be open for voting
    pub max_voting_time: u32,

    /// Conditions under which a vote will complete early
    pub vote_tipping: VoteTipping,

    /// The time period in seconds within which a Proposal can be still cancelled after being voted on
```

```rust
    /// Once cool off time expires Proposal can't be cancelled any longer and becomes a law
    /// Note: This field is not implemented in the current version
    pub proposal_cool_off_time: u32,

    /// Minimum council weight a governance token owner must possess to be able to create a proposal
    pub min_council_weight_to_create_proposal: u64,
}

```

- Call Stack

```
UnResolved
```

- description:
- link:
- alleviation:

Issue: 12: TypeConfusion

Category	Severity	Status
TypeConfusion	Critical	GitHub Link to be added.

- Location

governance/program/src/instruction.rs:32:69: 32:80

```
BorshSchema
governance/program/src/instruction.rs:32:69: 32:80
    BorshSchema
governance/program/src/instruction.rs:32:69: 32:80
    BorshSchema
governance/program/src/state/proposal_transaction.rs:30:1: 37:2
    pub struct InstructionData {
    /// Pubkey of the instruction processor that executes this instruction
    pub program_id: Pubkey,
    /// Metadata for what accounts should be passed to the instruction processor
    pub accounts: Vec<AccountMetaData>,
    /// Opaque data passed to the instruction processor
    pub data: Vec<u8>,
}
governance/program/src/state/proposal_transaction.rs:42:1: 49:2
    pub struct AccountMetaData {
    /// An account's public key
    pub pubkey: Pubkey,
    /// True if an Instruction requires a Transaction signature matching `pubkey`.
    pub is_signer: bool,
    /// True if the `pubkey` can be loaded as a read-write account.
    pub is_writable: bool,
}

```

- Call Stack

```
UnResolved
```

- description:
- link:
- alleviation:

Issue: 13: TypeConfusion

Category	Severity	Status
TypeConfusion	Critical	GitHub Link to be added.

- Location

governance/program/src/instruction.rs:32:69: 32:80

```
BorshSchema
governance/program/src/instruction.rs:32:69: 32:80
    BorshSchema
governance/program/src/state/proposal_transaction.rs:30:1: 37:2
    pub struct InstructionData {
    /// Pubkey of the instruction processor that executes this instruction
    pub program_id: Pubkey,
    /// Metadata for what accounts should be passed to the instruction processor
    pub accounts: Vec<AccountMetaData>,
    /// Opaque data passed to the instruction processor
    pub data: Vec<u8>,
}
governance/program/src/state/proposal_transaction.rs:42:1: 49:2
    pub struct AccountMetaData {
    /// An account's public key
    pub pubkey: Pubkey,
    /// True if an Instruction requires a Transaction signature matching `pubkey`.
    pub is_signer: bool,
    /// True if the `pubkey` can be loaded as a read-write account.
    pub is_writable: bool,
}

```

- Call Stack

```
UnResolved
```

- description:

- link:
- alleviation:

Issue: 14: TypeConfusion

Category	Severity	Status
TypeConfusion	Critical	GitHub Link to be added.

- Location

governance/program/src/instruction.rs:32:69: 32:80

```
BorshSchema
governance/program/src/state/proposal_transaction.rs:30:1: 37:2
    pub struct InstructionData {
    /// Pubkey of the instruction processor that executes this instruction
    pub program_id: Pubkey,
    /// Metadata for what accounts should be passed to the instruction processor
    pub accounts: Vec<AccountMetaData>,
    /// Opaque data passed to the instruction processor
    pub data: Vec<u8>,
}
governance/program/src/state/proposal_transaction.rs:42:1: 49:2
    pub struct AccountMetaData {
    /// An account's public key
    pub pubkey: Pubkey,
    /// True if an Instruction requires a Transaction signature matching `pubkey`.
    pub is_signer: bool,
    /// True if the `pubkey` can be loaded as a read-write account.
    pub is_writable: bool,
}

```

- Call Stack

```
UnResolved
```

- description:
- link:
- alleviation:

Issue: 15: TypeConfusion

Category	Severity	Status
TypeConfusion	Critical	GitHub Link to be added.

- Location

governance/program/src/instruction.rs:32:69: 32:80

```
BorshSchema
governance/program/src/state/enums.rs:142:69: 142:80
    BorshSchema
governance/program/src/state/enums.rs:142:69: 142:80
    BorshSchema
governance/program/src/state/proposal.rs:76:69: 76:80
    BorshSchema
governance/program/src/state/vote_record.rs:26:1: 33:2
    pub struct VoteChoice {
    /// The rank given to the choice by voter
    /// Note: The filed is not used in the current version
    pub rank: u8,

    /// The voter's weight percentage given by the voter to the choice
    pub weight_percentage: u8,
}
governance/program/src/instruction.rs:32:69: 32:80
    BorshSchema
governance/program/src/state/realm.rs:32:1: 50:2
    pub struct RealmConfigArgs {
    /// Indicates whether council_mint should be used
    /// If yes then council_mint account must also be passed to the
     ↪  instruction
    pub use_council_mint: bool,

    /// Min number of community tokens required to create a governance
    pub min_community_weight_to_create_governance: u64,

    /// The source used for community mint max vote weight source
    pub community_mint_max_vote_weight_source: MintMaxVoteWeightSource,

    /// Indicates whether an external addin program should be used to provide community voters weights
    /// If yes then the voters weight program account must be passed to the instruction
    pub use_community_voter_weight_addin: bool,

    /// Indicates whether an external addin program should be used to provide max voters weight for the community mint
    /// If yes then the max voter weight program account must be passed to the instruction
    pub use_max_community_voter_weight_addin: bool,
}
governance/program/src/state/realm.rs:71:1: 89:2
    pub struct RealmConfig {
    /// Indicates whether an external addin program should be used to provide voters weights for the community mint
    pub use_community_voter_weight_addin: bool,

    /// Indicates whether an external addin program should be used to provide max voter weight for the community mint
    pub use_max_community_voter_weight_addin: bool,

    /// Reserved space for future versions
    pub reserved: [u8; 6],

    /// Min number of voter's community weight required to create a governance
    pub min_community_weight_to_create_governance: u64,

    /// The source used for community mint max vote weight source
    pub community_mint_max_vote_weight_source: MintMaxVoteWeightSource,

    /// Optional council mint
    pub council_mint: Option<Pubkey>,
}

```

- Call Stack

```
UnResolved
```

- description:

- link:
- alleviation:

Issue: 16: TypeConfusion

Category	Severity	Status
TypeConfusion	Critical	GitHub Link to be added.

- Location

governance/program/src/state/enums.rs:142:69: 142:80

```
BorshSchema
governance/program/src/state/enums.rs:142:69: 142:80
    BorshSchema
governance/program/src/state/proposal.rs:76:69: 76:80
    BorshSchema
governance/program/src/state/vote_record.rs:26:1: 33:2
    pub struct VoteChoice {
    /// The rank given to the choice by voter
    /// Note: The filed is not used in the current version
    pub rank: u8,

    /// The voter's weight percentage given by the voter to the choice
    pub weight_percentage: u8,
}
governance/program/src/instruction.rs:32:69: 32:80
    BorshSchema
governance/program/src/state/realm.rs:32:1: 50:2
    pub struct RealmConfigArgs {
    /// Indicates whether council_mint should be used
    /// If yes then council_mint account must also be passed to the
     ↪ instruction
    pub use_council_mint: bool,

    /// Min number of community tokens required to create a governance
    pub min_community_weight_to_create_governance: u64,

    /// The source used for community mint max vote weight source
    pub community_mint_max_vote_weight_source: MintMaxVoteWeightSource,

    /// Indicates whether an external addin program should be used to
     ↪ provide community voters weights
    /// If yes then the voters weight program account must be passed to the instruction
    pub use_community_voter_weight_addin: bool,

    /// Indicates whether an external addin program should be used to provide max voters weight for the community mint
    /// If yes then the max voter weight program account must be passed to the instruction
    pub use_max_community_voter_weight_addin: bool,
}
governance/program/src/state/realm.rs:71:1: 89:2
    pub struct RealmConfig {
    /// Indicates whether an external addin program should be used to provide voters weights for the community mint
    pub use_community_voter_weight_addin: bool,

    /// Indicates whether an external addin program should be used to provide max voter weight for the community mint
    pub use_max_community_voter_weight_addin: bool,

    /// Reserved space for future versions
    pub reserved: [u8; 6],

    /// Min number of voter's community weight required to create a governance
    pub min_community_weight_to_create_governance: u64,

    /// The source used for community mint max vote weight source
    pub community_mint_max_vote_weight_source: MintMaxVoteWeightSource,

    /// Optional council mint
    pub council_mint: Option<Pubkey>,
}

```

- Call Stack

```
UnResolved
```

- description:
- link:

- alleviation:

Issue: 17: TypeConfusion

Category	Severity	Status
TypeConfusion	Critical	GitHub Link to be added.

- Location

governance/program/src/state/enums.rs:142:69: 142:80

```
BorshSchema
governance/program/src/state/proposal.rs:76:69: 76:80
    BorshSchema
governance/program/src/state/vote_record.rs:26:1: 33:2
    pub struct VoteChoice {
    /// The rank given to the choice by voter
    /// Note: The filed is not used in the current version
    pub rank: u8,

    /// The voter's weight percentage given by the voter to the choice
    pub weight_percentage: u8,
}
governance/program/src/instruction.rs:32:69: 32:80
    BorshSchema
governance/program/src/state/realm.rs:32:1: 50:2
    pub struct RealmConfigArgs {
    /// Indicates whether council_mint should be used
    /// If yes then council_mint account must also be passed to the instruction
    pub use_council_mint: bool,

    /// Min number of community tokens required to create a governance
    pub min_community_weight_to_create_governance: u64,

    /// The source used for community mint max vote weight source
    pub community_mint_max_vote_weight_source: MintMaxVoteWeightSource,

    /// Indicates whether an external addin program should be used to provide community voters weights
    /// If yes then the voters weight program account must be passed to the instruction
    pub use_community_voter_weight_addin: bool,

    /// Indicates whether an external addin program should be used to provide max voters weight for the community mint
    /// If yes then the max voter weight program account must be passed to the instruction
    pub use_max_community_voter_weight_addin: bool,
}
governance/program/src/state/realm.rs:71:1: 89:2
    pub struct RealmConfig {
    /// Indicates whether an external addin program should be used to provide voters weights for the community mint
    pub use_community_voter_weight_addin: bool,

    /// Indicates whether an external addin program should be used to provide max voter weight for the community mint
    pub use_max_community_voter_weight_addin: bool,

    /// Reserved space for future versions
    pub reserved: [u8; 6],

    /// Min number of voter's community weight required to create a governance
    pub min_community_weight_to_create_governance: u64,

    /// The source used for community mint max vote weight source
    pub community_mint_max_vote_weight_source: MintMaxVoteWeightSource,

    /// Optional council mint
    pub council_mint: Option<Pubkey>,
}

```

- Call Stack

```
UnResolved
```

- description:
- link:
- alleviation:

Issue: 18: TypeConfusion

Category	Severity	Status
TypeConfusion	Critical	GitHub Link to be added.

- Location

governance/program/src/state/enums.rs:215:69: 215:80

```
BorshSchema
governance/program/src/state/enums.rs:215:69: 215:80
    BorshSchema
governance/program/src/state/legacy.rs:322:69: 322:80
    BorshSchema
governance/program/src/state/legacy.rs:322:69: 322:80
    BorshSchema
governance/program/src/state/governance.rs:25:1: 49:2
    pub struct GovernanceConfig {
    /// The type of the vote threshold used for voting
    /// Note: In the current version only YesVote threshold is supported
    pub vote_threshold_percentage: VoteThresholdPercentage,

    /// Minimum community weight a governance token owner must possess to be able to create a proposal
    pub min_community_weight_to_create_proposal: u64,

    /// Minimum waiting time in seconds for a transaction to be executed after proposal is voted on
    pub min_transaction_hold_up_time: u32,

    /// Time limit in seconds for proposal to be open for voting
    pub max_voting_time: u32,

    /// Conditions under which a vote will complete early
    pub vote_tipping: VoteTipping,

    /// The time period in seconds within which a Proposal can be still cancelled after being voted on
    /// Once cool off time expires Proposal can't be cancelled any longer and becomes a law
```

```rust
    /// Note: This field is not implemented in the current version
    pub proposal_cool_off_time: u32,

    /// Minimum council weight a governance token owner must possess to be
    ↪  able to create a proposal
    pub min_council_weight_to_create_proposal: u64,
}

```

- Call Stack

```
UnResolved
```

- description:
- link:
- alleviation:

Issue: 19: TypeConfusion

Category	Severity	Status
TypeConfusion	Critical	GitHub Link to be added.

- Location

governance/program/src/state/enums.rs:215:69: 215:80

```
BorshSchema
governance/program/src/state/legacy.rs:322:69: 322:80
    BorshSchema
governance/program/src/state/legacy.rs:322:69: 322:80
    BorshSchema
governance/program/src/state/governance.rs:25:1: 49:2
    pub struct GovernanceConfig {
    /// The type of the vote threshold used for voting
    /// Note: In the current version only YesVote threshold is supported
    pub vote_threshold_percentage: VoteThresholdPercentage,

    /// Minimum community weight a governance token owner must possess to be able to create a proposal
    pub min_community_weight_to_create_proposal: u64,

    /// Minimum waiting time in seconds for a transaction to be executed after proposal is voted on
    pub min_transaction_hold_up_time: u32,

    /// Time limit in seconds for proposal to be open for voting
    pub max_voting_time: u32,

    /// Conditions under which a vote will complete early
    pub vote_tipping: VoteTipping,

    /// The time period in seconds within which a Proposal can be still cancelled after being voted on
    /// Once cool off time expires Proposal can't be cancelled any longer and becomes a law
    /// Note: This field is not implemented in the current version
    pub proposal_cool_off_time: u32,

    /// Minimum council weight a governance token owner must possess to be able to create a proposal
    pub min_council_weight_to_create_proposal: u64,
}

```

- Call Stack

```
UnResolved
```

- description:
- link:
- alleviation:

Issue: 20: TypeConfusion

Category	Severity	Status
TypeConfusion	Critical	GitHub Link to be added.

- Location

governance/program/src/state/legacy.rs:322:69: 322:80

```
BorshSchema
governance/program/src/state/legacy.rs:322:69: 322:80
    BorshSchema
governance/program/src/state/governance.rs:25:1: 49:2
    pub struct GovernanceConfig {
    /// The type of the vote threshold used for voting
    /// Note: In the current version only YesVote threshold is supported
    pub vote_threshold_percentage: VoteThresholdPercentage,

    /// Minimum community weight a governance token owner must possess to be able to create a proposal
    pub min_community_weight_to_create_proposal: u64,

    /// Minimum waiting time in seconds for a transaction to be executed after proposal is voted on
    pub min_transaction_hold_up_time: u32,

    /// Time limit in seconds for proposal to be open for voting
    pub max_voting_time: u32,

    /// Conditions under which a vote will complete early
    pub vote_tipping: VoteTipping,

    /// The time period in seconds within which a Proposal can be still cancelled after being voted on
    /// Once cool off time expires Proposal can't be cancelled any longer and becomes a law
    /// Note: This field is not implemented in the current version
    pub proposal_cool_off_time: u32,

    /// Minimum council weight a governance token owner must possess to be able to create a proposal
    pub min_council_weight_to_create_proposal: u64,
}

```

- Call Stack

```
UnResolved
```

- description:
- link:
- alleviation:

Issue: 21: TypeConfusion

Category	Severity	Status
TypeConfusion	Critical	GitHub Link to be added.

- Location

governance/program/src/state/legacy.rs:322:69: 322:80

```
BorshSchema
governance/program/src/state/governance.rs:25:1: 49:2
    pub struct GovernanceConfig {
    /// The type of the vote threshold used for voting
    /// Note: In the current version only YesVote threshold is supported
    pub vote_threshold_percentage: VoteThresholdPercentage,

    /// Minimum community weight a governance token owner must possess to be able to create a proposal
    pub min_community_weight_to_create_proposal: u64,

    /// Minimum waiting time in seconds for a transaction to be executed after proposal is voted on
    pub min_transaction_hold_up_time: u32,

    /// Time limit in seconds for proposal to be open for voting
    pub max_voting_time: u32,

    /// Conditions under which a vote will complete early
    pub vote_tipping: VoteTipping,

    /// The time period in seconds within which a Proposal can be still cancelled after being voted on
    /// Once cool off time expires Proposal can't be cancelled any longer and becomes a law
    /// Note: This field is not implemented in the current version
    pub proposal_cool_off_time: u32,

    /// Minimum council weight a governance token owner must possess to be able to create a proposal
    pub min_council_weight_to_create_proposal: u64,
}

```

- Call Stack

```
UnResolved
```

- description:
- link:
- alleviation:

Issue: 22: TypeConfusion

Category	Severity	Status
TypeConfusion	Critical	GitHub Link to be added.

- Location

governance/program/src/state/proposal.rs:76:69: 76:80

```
BorshSchema
governance/program/src/state/vote_record.rs:26:1: 33:2
    pub struct VoteChoice {
    /// The rank given to the choice by voter
    /// Note: The filed is not used in the current version
    pub rank: u8,

    /// The voter's weight percentage given by the voter to the choice
    pub weight_percentage: u8,
}
governance/program/src/state/realm.rs:71:1: 89:2
    pub struct RealmConfig {
    /// Indicates whether an external addin program should be used to provide voters weights for the community mint
    pub use_community_voter_weight_addin: bool,

    /// Indicates whether an external addin program should be used to provide max voter weight for the community mint
    pub use_max_community_voter_weight_addin: bool,

    /// Reserved space for future versions
    pub reserved: [u8; 6],

    /// Min number of voter's community weight required to create a governance
    pub min_community_weight_to_create_governance: u64,

    /// The source used for community mint max vote weight source
    pub community_mint_max_vote_weight_source: MintMaxVoteWeightSource,

    /// Optional council mint
    pub council_mint: Option<Pubkey>,
}

```

- Call Stack

```
UnResolved
```

- description:
- link:
- alleviation:

Issue: 23: TypeConfusion

Category	Severity	Status
TypeConfusion	Critical	GitHub Link to be added.

- Location

governance/program/src/state/vote_record.rs:26:1: 33:2

```
pub struct VoteChoice {
    /// The rank given to the choice by voter
    /// Note: The filed is not used in the current version
    pub rank: u8,

    /// The voter's weight percentage given by the voter to the choice
    pub weight_percentage: u8,
}
governance/program/src/state/realm.rs:71:1: 89:2
    pub struct RealmConfig {
    /// Indicates whether an external addin program should be used to provide voters weights for the community mint
    pub use_community_voter_weight_addin: bool,

    /// Indicates whether an external addin program should be used to provide max voter weight for the community mint
    pub use_max_community_voter_weight_addin: bool,

    /// Reserved space for future versions
    pub reserved: [u8; 6],

    /// Min number of voter's community weight required to create a governance
    pub min_community_weight_to_create_governance: u64,

    /// The source used for community mint max vote weight source
    pub community_mint_max_vote_weight_source: MintMaxVoteWeightSource,

    /// Optional council mint
    pub council_mint: Option<Pubkey>,
}
```

```

```

- Call Stack

```
UnResolved
```

- 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.