



VRust

Security Assessment

O2Lab VRust Team

11/04/2022 17:27:41

Contents

Summary	4
Overview	5
Project Summary	5
Audit Summary	5
Vulnerability Summary	5
Findings	6
Finding Statistic	7
Issue: 0: MissingKeyCheck	9
Issue: 1: MissingKeyCheck	11
Issue: 2: MissingKeyCheck	13
Issue: 3: MissingKeyCheck	15
Issue: 4: MissingKeyCheck	17
Issue: 5: MissingKeyCheck	19
Issue: 6: MissingKeyCheck	21
Issue: 7: MissingKeyCheck	23
Issue: 8: MissingKeyCheck	25
Issue: 9: MissingKeyCheck	27
Issue: 10: MissingKeyCheck	29
Issue: 11: TypeConfusion	31
Issue: 12: TypeConfusion	33
Issue: 13: TypeConfusion	35
Issue: 14: TypeConfusion	37
Issue: 15: TypeConfusion	38

Issue: 16: TypeConfusion	41
Issue: 17: TypeConfusion	44
Issue: 18: TypeConfusion	46
Issue: 19: TypeConfusion	48
Issue: 20: TypeConfusion	50
Issue: 21: TypeConfusion	52
Issue: 22: TypeConfusion	54
Issue: 23: TypeConfusion	56
Appendix	58
Finding Categories	58
Gas Optimization	58
Mathematical Operations	58
Logical Issue	58
Language Specific	58
Coding Style	58
Checksum Calculation Method	58
Disclaimer	60

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

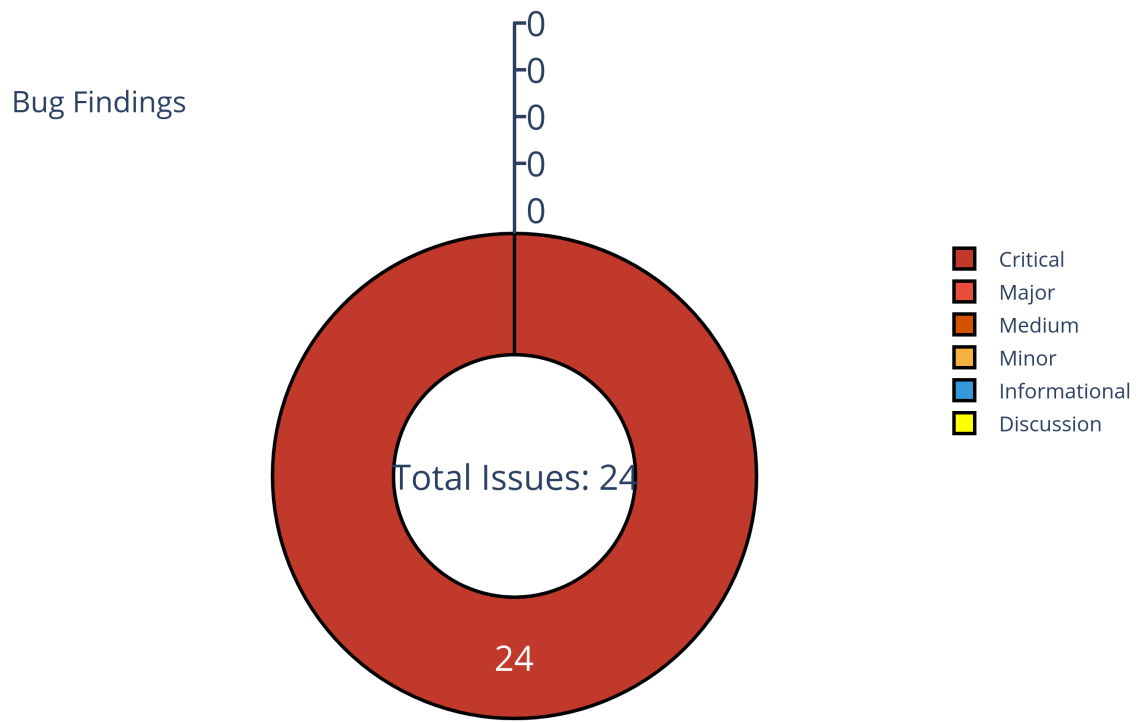


Figure 1: Findings

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

```
66 self.lamports.borrow()
```

```
67
```

- Code Context

Vulnerability at Line: 66

```
65 pub fn lamports(&self) -> u64 {
66     **self.lamports.borrow()
67 }
68
```

- Call Stack

```
1 fn entrypoint::process_instruction() { //
  ↳ governance/program/src/entrypoint.rs:11:1: 22:2 }
2   fn processor::process_instruction() { //
  ↳ governance/program/src/processor/mod.rs:65:1: 217:2 }
3   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 }
4   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
  ↳ }
5   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
  ↳ }
```

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

```

1  fn entrypoint::process_instruction() {
  ↪  governance/program/src/entrypoint.rs:11:1: 22:2 }
2  fn processor::process_instruction() {
  ↪  governance/program/src/processor/mod.rs:65:1: 217:2 }
3  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 }

```

4

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  
↳ }
```

5

- 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 =
299         ↪ try_from_slice_unchecked(&realm_info.data.borrow())?;
300
301     // If the account is V1 version then translate to V2
302     if account_type == GovernanceAccountType::RealmV1 {
303         let realm_data_v1 = get_account_data::<RealmV1>(program_id,
304             ↪ realm_info)?;
```

- Call Stack

```
1 fn entrypoint::process_instruction() {
  ↪ governance/program/src/entrypoint.rs:11:1: 22:2 }
2 fn processor::process_instruction() {
  ↪ governance/program/src/processor/mod.rs:65:1: 217:2 }
3 fn proces-
  ↪ sor::process_create_token_owner_record::process_create_token_owner_record() {
  ↪ gover-
  ↪ nance/program/src/processor/process_create_token_owner_record.rs:22:1:
  ↪ 70:2 }
4 fn state::realm::get_realm_data() {
  ↪ governance/program/src/state/realm.rs:294:1: 318:2 }
```

5

- 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,
853             ↪ proposal_info)?;
```

- Call Stack

```
1 fn entrypoint::process_instruction() {
  ↪ governance/program/src/entrypoint.rs:11:1: 22:2 }
2 fn processor::process_instruction() {
  ↪ governance/program/src/processor/mod.rs:65:1: 217:2 }
3 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 }
4 fn state::proposal::get_proposal_data() {
  ↪ governance/program/src/state/proposal.rs:843:1: 905:2 }
```

5

- 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
214     ↪ try_from_slice_unchecked(&proposal_transaction_info.data.borrow())?;
215
216     // If the account is V1 version then translate to V2
217     if account_type == GovernanceAccountType::ProposalInstructionV1 {
218         let proposal_transaction_data_v1 =
```

- Call Stack

```
1 fn entrypoint::process_instruction() {
2     ↪ governance/program/src/entrypoint.rs:11:1: 22:2 }
3     fn processor::process_instruction() {
4         ↪ governance/program/src/processor/mod.rs:65:1: 217:2 }
5         fn proces-
6             ↪ sor::process_flag_transaction_error::process_flag_transaction_error() {
7             ↪ gover-
8             ↪ nance/program/src/processor/process_flag_transaction_error.rs:19:1:
9             ↪ 65:2 }
10        fn
11            ↪ state::proposal_transaction::get_proposal_transaction_data_for_proposal(
12            ↪ governance/program/src/state/proposal_transaction.rs:237:1:
13            ↪ 250:2 }
```

5

fn

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

6

- 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
95     ↪ well
96     let token_account_data =
97     ↪ Account::unpack(&governed_token_info.data.borrow())?;
98     // Note: The code assumes owner==close_authority
99     // If this is not the case then the caller should set
100    ↪ close_authority accordingly before making the transfer
    if token_account_data.close_authority.is_some() {
        set_spl_token_account_authority(

```

- Call Stack

```

1  fn entrypoint::process_instruction() {
2  ↪ governance/program/src/entrypoint.rs:11:1: 22:2 }
3  fn processor::process_instruction() {
4  ↪ governance/program/src/processor/mod.rs:65:1: 217:2 }
5  fn proces-
6  ↪ sor::process_create_token_governance::process_create_token_governance() {
7  ↪ gover-
8  ↪ nance/program/src/processor/process_create_token_governance.rs:27:1:
9  ↪ 112:2 }

```

4

- 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

```

97 governed_mint_info.data.borrow()
98

```

- Code Context

Vulnerability at Line: 97

```

92     AuthorityType::MintTokens,
93     spl_token_info,
94 )?;
95
96 // If the mint has freeze_authority then transfer it as well
97 let mint_data = Mint::unpack(&governed_mint_info.data.borrow())?;
98 // Note: The code assumes mint_authority==freeze_authority
99 //       If this is not the case then the caller should set
100 ↪ freeze_authority accordingly before making the transfer
101 if mint_data.freeze_authority.is_some() {
102     set_spl_token_account_authority(

```

- Call Stack

```

1 fn entrypoint::process_instruction() {
  ↪ governance/program/src/entrypoint.rs:11:1: 22:2 }
2 fn processor::process_instruction() {
  ↪ governance/program/src/processor/mod.rs:65:1: 217:2 }
3 fn proces-
  ↪ sor::process_create_mint_governance::process_create_mint_governance() {
  ↪ gover-
  ↪ nance/program/src/processor/process_create_mint_governance.rs:29:1:
  ↪ 117:2 }
4

```

-
- 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 =
154             ↪ get_account_data::<VoteRecordV1>(program_id,
155             ↪ vote_record_info)?;
```

- Call Stack

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

5

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

6

- 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

```
1 fn entrypoint::process_instruction() {
  ↳ governance/program/src/entrypoint.rs:11:1: 22:2 }
2 fn processor::process_instruction() {
  ↳ governance/program/src/processor/mod.rs:65:1: 217:2 }
3 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 }
4 fn
  ↳ state::signatory_record::get_signatory_record_data_for_seeds() {
  ↳ governance/program/src/state/signatory_record.rs:151:1:
  ↳ 167:2 }
```

5

fn

```
↳ state::signatory_record::get_signatory_record_data() { //  
↳ gover-  
↳ nance/program/src/state/signatory_record.rs:123:1:  
↳ 148:2 }
```

6

- 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

```
1 fn entrypoint::process_instruction() {
↳ governance/program/src/entrypoint.rs:11:1: 22:2 }
2 fn processor::process_instruction() {
↳ governance/program/src/processor/mod.rs:65:1: 217:2 }
3     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 }
4
```

-
- 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

```
73 token_owner_record_info.data.borrow_mut()
74
```

- Code Context

Vulnerability at Line: 73

```
68         token_owner_record_data.governing_token_deposit_amount,
69         spl_token_info,
70     )?;
71
72     token_owner_record_data.governing_token_deposit_amount = 0;
73     token_owner_record_data.serialize(&mut
↳ *token_owner_record_info.data.borrow_mut())?;
74
75     Ok(())
76 }
77
```

- Call Stack

```
1 fn entrypoint::process_instruction() {
↳ governance/program/src/entrypoint.rs:11:1: 22:2 }
2 fn processor::process_instruction() {
↳ governance/program/src/processor/mod.rs:65:1: 217:2 }
3     fn proces-
↳ sor::process_withdraw_governing_tokens::process_withdraw_governing_tokens() {
↳ gover-
↳ nance/program/src/processor/process_withdraw_governing_tokens.rs:21:1:
↳ 76:2 }
4
```

- 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

```

32 BorshSchema
33 governance/program/src/state/enums.rs:215:69: 215:80
34     BorshSchema
35 governance/program/src/state/enums.rs:215:69: 215:80
36     BorshSchema
37 governance/program/src/state/legacy.rs:322:69: 322:80
38     BorshSchema
39 governance/program/src/state/legacy.rs:322:69: 322:80
40     BorshSchema
41 governance/program/src/state/governance.rs:25:1: 49:2
42     pub struct GovernanceConfig {
43         /// The type of the vote threshold used for voting
44         /// Note: In the current version only YesVote threshold is supported
45         pub vote_threshold_percentage: VoteThresholdPercentage,
46
47         /// Minimum community weight a governance token owner must possess to
48         ↪ be able to create a proposal
49         pub min_community_weight_to_create_proposal: u64,
50
51         /// Minimum waiting time in seconds for a transaction to be executed
52         ↪ after proposal is voted on
53         pub min_transaction_hold_up_time: u32,
54
55         /// Time limit in seconds for proposal to be open for voting
56         pub max_voting_time: u32,
57
58         /// Conditions under which a vote will complete early
59         pub vote_tipping: VoteTipping,
60
61         /// The time period in seconds within which a Proposal can be still
62         ↪ cancelled after being voted on

```

```
60    /// Once cool off time expires Proposal can't be cancelled any longer
    ↪ and becomes a law
61    /// Note: This field is not implemented in the current version
62    pub proposal_cool_off_time: u32,
63
64    /// Minimum council weight a governance token owner must possess to be
    ↪ able to create a proposal
65    pub min_council_weight_to_create_proposal: u64,
66 }
67
```

- Call Stack

1 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

```
32 BorshSchema
33 governance/program/src/instruction.rs:32:69: 32:80
34     BorshSchema
35 governance/program/src/instruction.rs:32:69: 32:80
36     BorshSchema
37 governance/program/src/state/proposal_transaction.rs:30:1: 37:2
38     pub struct InstructionData {
39         /// Pubkey of the instruction processor that executes this instruction
40         pub program_id: Pubkey,
41         /// Metadata for what accounts should be passed to the instruction
42         ↪ processor
43         pub accounts: Vec<AccountMetaData>,
44         /// Opaque data passed to the instruction processor
45         pub data: Vec<u8>,
46     }
47 governance/program/src/state/proposal_transaction.rs:42:1: 49:2
48     pub struct AccountMetaData {
49         /// An account's public key
50         pub pubkey: Pubkey,
51         /// True if an Instruction requires a Transaction signature matching
52         ↪ `pubkey`.
53         pub is_signer: bool,
54         /// True if the `pubkey` can be loaded as a read-write account.
55         pub is_writable: bool,
56     }
```

- Call Stack

1 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

```
32 BorshSchema
33 governance/program/src/instruction.rs:32:69: 32:80
34     BorshSchema
35 governance/program/src/state/proposal_transaction.rs:30:1: 37:2
36     pub struct InstructionData {
37         /// Pubkey of the instruction processor that executes this instruction
38         pub program_id: Pubkey,
39         /// Metadata for what accounts should be passed to the instruction
40         ↪ processor
41         pub accounts: Vec<AccountMetaData>,
42         /// Opaque data passed to the instruction processor
43         pub data: Vec<u8>,
44     }
45 governance/program/src/state/proposal_transaction.rs:42:1: 49:2
46     pub struct AccountMetaData {
47         /// An account's public key
48         pub pubkey: Pubkey,
49         /// True if an Instruction requires a Transaction signature matching
50         ↪ `pubkey`.
51         pub is_signer: bool,
52         /// True if the `pubkey` can be loaded as a read-write account.
53         pub is_writable: bool,
54     }
```

- Call Stack

1 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

```

32 BorshSchema
33 governance/program/src/state/proposal_transaction.rs:30:1: 37:2
34     pub struct InstructionData {
35         /// Pubkey of the instruction processor that executes this instruction
36         pub program_id: Pubkey,
37         /// Metadata for what accounts should be passed to the instruction
38         ↳ processor
39         pub accounts: Vec<AccountMetaData>,
40         /// Opaque data passed to the instruction processor
41         pub data: Vec<u8>,
42     }
43 governance/program/src/state/proposal_transaction.rs:42:1: 49:2
44     pub struct AccountMetaData {
45         /// An account's public key
46         pub pubkey: Pubkey,
47         /// True if an Instruction requires a Transaction signature matching
48         ↳ `pubkey`.
49         pub is_signer: bool,
50         /// True if the `pubkey` can be loaded as a read-write account.
51         pub is_writable: bool,
52     }

```

- Call Stack

1 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

```

32 BorshSchema
33 governance/program/src/state/enums.rs:142:69: 142:80
34     BorshSchema
35 governance/program/src/state/enums.rs:142:69: 142:80
36     BorshSchema
37 governance/program/src/state/proposal.rs:76:69: 76:80
38     BorshSchema
39 governance/program/src/state/vote_record.rs:26:1: 33:2
40     pub struct VoteChoice {
41         /// The rank given to the choice by voter
42         /// Note: The field is not used in the current version
43         pub rank: u8,
44
45         /// The voter's weight percentage given by the voter to the choice
46         pub weight_percentage: u8,
47     }
48 governance/program/src/instruction.rs:32:69: 32:80
49     BorshSchema
50 governance/program/src/state/realm.rs:32:1: 50:2
51     pub struct RealmConfigArgs {
52         /// Indicates whether council_mint should be used
53         /// If yes then council_mint account must also be passed to the
54         ↪ instruction
55         pub use_council_mint: bool,
56
57         /// Min number of community tokens required to create a governance
58         pub min_community_weight_to_create_governance: u64,
59
60         /// The source used for community mint max vote weight source
61         pub community_mint_max_vote_weight_source: MintMaxVoteWeightSource,

```

```

62    /// Indicates whether an external addin program should be used to
63    ↪ provide community voters weights
64    /// If yes then the voters weight program account must be passed to the
65    ↪ instruction
66    pub use_community_voter_weight_addin: bool,
67
68    /// Indicates whether an external addin program should be used to
69    ↪ provide max voters weight for the community mint
70    /// If yes then the max voter weight program account must be passed to
71    ↪ the instruction
72    pub use_max_community_voter_weight_addin: bool,
73 }
74 governance/program/src/state/realm.rs:71:1: 89:2
75 pub struct RealmConfig {
76    /// Indicates whether an external addin program should be used to
77    ↪ provide voters weights for the community mint
78    pub use_community_voter_weight_addin: bool,
79
80    /// Indicates whether an external addin program should be used to
81    ↪ provide max voter weight for the community mint
82    pub use_max_community_voter_weight_addin: bool,
83
84    /// Reserved space for future versions
85    pub reserved: [u8; 6],
86
87    /// Min number of voter's community weight required to create a
88    ↪ governance
89    pub min_community_weight_to_create_governance: u64,
90
91    /// The source used for community mint max vote weight source
92    pub community_mint_max_vote_weight_source: MintMaxVoteWeightSource,
93
94    /// Optional council mint
95    pub council_mint: Option<Pubkey>,
96 }

```

- Call Stack

1 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

```

142 BorshSchema
143 governance/program/src/state/enums.rs:142:69: 142:80
144     BorshSchema
145 governance/program/src/state/proposal.rs:76:69: 76:80
146     BorshSchema
147 governance/program/src/state/vote_record.rs:26:1: 33:2
148     pub struct VoteChoice {
149         /// The rank given to the choice by voter
150         /// Note: The filed is not used in the current version
151         pub rank: u8,
152
153         /// The voter's weight percentage given by the voter to the choice
154         pub weight_percentage: u8,
155     }
156 governance/program/src/instruction.rs:32:69: 32:80
157     BorshSchema
158 governance/program/src/state/realm.rs:32:1: 50:2
159     pub struct RealmConfigArgs {
160         /// Indicates whether council_mint should be used
161         /// If yes then council_mint account must also be passed to the
162         ↳ instruction
163         pub use_council_mint: bool,
164
165         /// Min number of community tokens required to create a governance
166         pub min_community_weight_to_create_governance: u64,
167
168         /// The source used for community mint max vote weight source
169         pub community_mint_max_vote_weight_source: MintMaxVoteWeightSource,
170
171         /// Indicates whether an external addin program should be used to
172         ↳ provide community voters weights

```

```

171    /// If yes then the voters weight program account must be passed to the
172    ↪ instruction
173    pub use_community_voter_weight_addin: bool,
174
175    /// Indicates whether an external addin program should be used to
176    ↪ provide max voters weight for the community mint
177    /// If yes then the max voter weight program account must be passed to
178    ↪ the instruction
179    pub use_max_community_voter_weight_addin: bool,
180 }
181 governance/program/src/state/realm.rs:71:1: 89:2
182 pub struct RealmConfig {
183     /// Indicates whether an external addin program should be used to
184     ↪ provide voters weights for the community mint
185     pub use_community_voter_weight_addin: bool,
186
187     /// Indicates whether an external addin program should be used to
188     ↪ provide max voter weight for the community mint
189     pub use_max_community_voter_weight_addin: bool,
190
191     /// Reserved space for future versions
192     pub reserved: [u8; 6],
193
194     /// Min number of voter's community weight required to create a
195     ↪ governance
196     pub min_community_weight_to_create_governance: u64,
197
198     /// The source used for community mint max vote weight source
199     pub community_mint_max_vote_weight_source: MintMaxVoteWeightSource,
200
201     /// Optional council mint
202     pub council_mint: Option<Pubkey>,
203 }

```

- Call Stack

1 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

```

142 BorshSchema
143 governance/program/src/state/proposal.rs:76:69: 76:80
144     BorshSchema
145 governance/program/src/state/vote_record.rs:26:1: 33:2
146     pub struct VoteChoice {
147         /// The rank given to the choice by voter
148         /// Note: The field is not used in the current version
149         pub rank: u8,
150
151         /// The voter's weight percentage given by the voter to the choice
152         pub weight_percentage: u8,
153     }
154 governance/program/src/instruction.rs:32:69: 32:80
155     BorshSchema
156 governance/program/src/state/realm.rs:32:1: 50:2
157     pub struct RealmConfigArgs {
158         /// Indicates whether council_mint should be used
159         /// If yes then council_mint account must also be passed to the
160         ↪ instruction
161         pub use_council_mint: bool,
162
163         /// Min number of community tokens required to create a governance
164         pub min_community_weight_to_create_governance: u64,
165
166         /// The source used for community mint max vote weight source
167         pub community_mint_max_vote_weight_source: MintMaxVoteWeightSource,
168
169         /// Indicates whether an external addin program should be used to
170         ↪ provide community voters weights
171         /// If yes then the voters weight program account must be passed to the
172         ↪ instruction

```

```

170     pub use_community_voter_weight_addin: bool,
171
172     /// Indicates whether an external addin program should be used to
173     ↪ provide max voters weight for the community mint
174     /// If yes then the max voter weight program account must be passed to
175     ↪ the instruction
176     pub use_max_community_voter_weight_addin: bool,
177 }
178 governance/program/src/state/realm.rs:71:1: 89:2
179 pub struct RealmConfig {
180     /// Indicates whether an external addin program should be used to
181     ↪ provide voters weights for the community mint
182     pub use_community_voter_weight_addin: bool,
183
184     /// Indicates whether an external addin program should be used to
185     ↪ provide max voter weight for the community mint
186     pub use_max_community_voter_weight_addin: bool,
187
188     /// Reserved space for future versions
189     pub reserved: [u8; 6],
190
191     /// Min number of voter's community weight required to create a
192     ↪ governance
193     pub min_community_weight_to_create_governance: u64,
194
195     /// The source used for community mint max vote weight source
196     pub community_mint_max_vote_weight_source: MintMaxVoteWeightSource,
197
198     /// Optional council mint
199     pub council_mint: Option<Pubkey>,
200 }

```

- Call Stack

1 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

```

215 BorshSchema
216 governance/program/src/state/enums.rs:215:69: 215:80
217     BorshSchema
218 governance/program/src/state/legacy.rs:322:69: 322:80
219     BorshSchema
220 governance/program/src/state/legacy.rs:322:69: 322:80
221     BorshSchema
222 governance/program/src/state/governance.rs:25:1: 49:2
223     pub struct GovernanceConfig {
224         /// The type of the vote threshold used for voting
225         /// Note: In the current version only YesVote threshold is supported
226         pub vote_threshold_percentage: VoteThresholdPercentage,
227
228         /// Minimum community weight a governance token owner must possess to
229         ↪ be able to create a proposal
230         pub min_community_weight_to_create_proposal: u64,
231
232         /// Minimum waiting time in seconds for a transaction to be executed
233         ↪ after proposal is voted on
234         pub min_transaction_hold_up_time: u32,
235
236         /// Time limit in seconds for proposal to be open for voting
237         pub max_voting_time: u32,
238
239         /// Conditions under which a vote will complete early
240         pub vote_tipping: VoteTipping,
241
242         /// The time period in seconds within which a Proposal can be still
243         ↪ cancelled after being voted on
244         /// Once cool off time expires Proposal can't be cancelled any longer
245         ↪ and becomes a law

```

```
242    /// Note: This field is not implemented in the current version
243    pub proposal_cool_off_time: u32,
244
245    /// Minimum council weight a governance token owner must possess to be
246    ↪ able to create a proposal
247    pub min_council_weight_to_create_proposal: u64,
248 }
```

- Call Stack

1 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

```

215 BorshSchema
216 governance/program/src/state/legacy.rs:322:69: 322:80
217     BorshSchema
218 governance/program/src/state/legacy.rs:322:69: 322:80
219     BorshSchema
220 governance/program/src/state/governance.rs:25:1: 49:2
221     pub struct GovernanceConfig {
222         /// The type of the vote threshold used for voting
223         /// Note: In the current version only YesVote threshold is supported
224         pub vote_threshold_percentage: VoteThresholdPercentage,
225
226         /// Minimum community weight a governance token owner must possess to
227         ↪ be able to create a proposal
228         pub min_community_weight_to_create_proposal: u64,
229
230         /// Minimum waiting time in seconds for a transaction to be executed
231         ↪ after proposal is voted on
232         pub min_transaction_hold_up_time: u32,
233
234         /// Time limit in seconds for proposal to be open for voting
235         pub max_voting_time: u32,
236
237         /// Conditions under which a vote will complete early
238         pub vote_tipping: VoteTipping,
239
240         /// The time period in seconds within which a Proposal can be still
241         ↪ cancelled after being voted on
242         /// Once cool off time expires Proposal can't be cancelled any longer
243         ↪ and becomes a law
244         /// Note: This field is not implemented in the current version
245         pub proposal_cool_off_time: u32,

```



```
242  
243     /// Minimum council weight a governance token owner must possess to be  
244     ↔ able to create a proposal  
244     pub min_council_weight_to_create_proposal: u64,  
245 }  
246
```

- Call Stack

1 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

```

322 BorshSchema
323 governance/program/src/state/legacy.rs:322:69: 322:80
324     BorshSchema
325 governance/program/src/state/governance.rs:25:1: 49:2
326     pub struct GovernanceConfig {
327         /// The type of the vote threshold used for voting
328         /// Note: In the current version only YesVote threshold is supported
329         pub vote_threshold_percentage: VoteThresholdPercentage,
330
331         /// Minimum community weight a governance token owner must possess to
332         ↳ be able to create a proposal
333         pub min_community_weight_to_create_proposal: u64,
334
335         /// Minimum waiting time in seconds for a transaction to be executed
336         ↳ after proposal is voted on
337         pub min_transaction_hold_up_time: u32,
338
339         /// Time limit in seconds for proposal to be open for voting
340         pub max_voting_time: u32,
341
342         /// Conditions under which a vote will complete early
343         pub vote_tipping: VoteTipping,
344
345         /// The time period in seconds within which a Proposal can be still
346         ↳ cancelled after being voted on
347         /// Once cool off time expires Proposal can't be cancelled any longer
348         ↳ and becomes a law
349         /// Note: This field is not implemented in the current version
350         pub proposal_cool_off_time: u32,
351
352         /// Minimum council weight a governance token owner must possess to be
353         ↳ able to create a proposal

```

```
349     pub min_council_weight_to_create_proposal: u64,  
350 }  
351
```

- Call Stack

1 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

```

322 BorshSchema
323 governance/program/src/state/governance.rs:25:1: 49:2
324     pub struct GovernanceConfig {
325         /// The type of the vote threshold used for voting
326         /// Note: In the current version only YesVoteThreshold is supported
327         pub vote_threshold_percentage: VoteThresholdPercentage,
328
329         /// Minimum community weight a governance token owner must possess to
330         ↳ be able to create a proposal
331         pub min_community_weight_to_create_proposal: u64,
332
333         /// Minimum waiting time in seconds for a transaction to be executed
334         ↳ after proposal is voted on
335         pub min_transaction_hold_up_time: u32,
336
337         /// Time limit in seconds for proposal to be open for voting
338         pub max_voting_time: u32,
339
340         /// Conditions under which a vote will complete early
341         pub vote_tipping: VoteTipping,
342
343         /// The time period in seconds within which a Proposal can be still
344         ↳ cancelled after being voted on
345         /// Once cool off time expires Proposal can't be cancelled any longer
346         ↳ and becomes a law
347         /// Note: This field is not implemented in the current version
348         pub proposal_cool_off_time: u32,
349
350         /// Minimum council weight a governance token owner must possess to be
351         ↳ able to create a proposal
352         pub min_council_weight_to_create_proposal: u64,
```

348

}

349

- Call Stack

1

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

```

76 BorshSchema
77 governance/program/src/state/vote_record.rs:26:1: 33:2
78     pub struct VoteChoice {
79         /// The rank given to the choice by voter
80         /// Note: The filed is not used in the current version
81         pub rank: u8,
82
83         /// The voter's weight percentage given by the voter to the choice
84         pub weight_percentage: u8,
85     }
86 governance/program/src/state/realm.rs:71:1: 89:2
87     pub struct RealmConfig {
88         /// Indicates whether an external addin program should be used to
89         ↪ provide voters weights for the community mint
90         pub use_community_voter_weight_addin: bool,
91
92         /// Indicates whether an external addin program should be used to
93         ↪ provide max voter weight for the community mint
94         pub use_max_community_voter_weight_addin: bool,
95
96         /// Reserved space for future versions
97         pub reserved: [u8; 6],
98
99         /// Min number of voter's community weight required to create a
100         ↪ governance
101         pub min_community_weight_to_create_governance: u64,
102
103         /// The source used for community mint max vote weight source
104         pub community_mint_max_vote_weight_source: MintMaxVoteWeightSource,
105
106         /// Optional council mint

```

```
104 pub council_mint: Option<Pubkey>,  
105 }  
106
```

- Call Stack

1 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

```

26 pub struct VoteChoice {
27     /// The rank given to the choice by voter
28     /// Note: The filed is not used in the current version
29     pub rank: u8,
30
31     /// The voter's weight percentage given by the voter to the choice
32     pub weight_percentage: u8,
33 }
34 governance/program/src/state/realms.rs:71:1: 89:2
35 pub struct RealmConfig {
36     /// Indicates whether an external addin program should be used to
37     ↪ provide voters weights for the community mint
38     pub use_community_voter_weight_addin: bool,
39
40     /// Indicates whether an external addin program should be used to
41     ↪ provide max voter weight for the community mint
42     pub use_max_community_voter_weight_addin: bool,
43
44     /// Reserved space for future versions
45     pub reserved: [u8; 6],
46
47     /// Min number of voter's community weight required to create a
48     ↪ governance
49     pub min_community_weight_to_create_governance: u64,
50
51     /// The source used for community mint max vote weight source
52     pub community_mint_max_vote_weight_source: MintMaxVoteWeightSource,
53
54     /// Optional council mint
55     pub council_mint: Option<Pubkey>,
56 }

```


54

- Call Stack

1 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.