VRust

Security Assessment

O2Lab VRust Team

15/02/2022 21:23:06

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	level1
GitHub Location	https://github.com/parasol-aser/vrust
sha256	Unknown

Audit Summary

Delivery Date	15/02/2022
Audit Methodology	Static Analysis
Key Components	

Vulnerability Summary

Vulnerability Level	Total
Critical	13
Major	0
Medium	0
Minor	0
Informational	0
Discussion	0

Findings

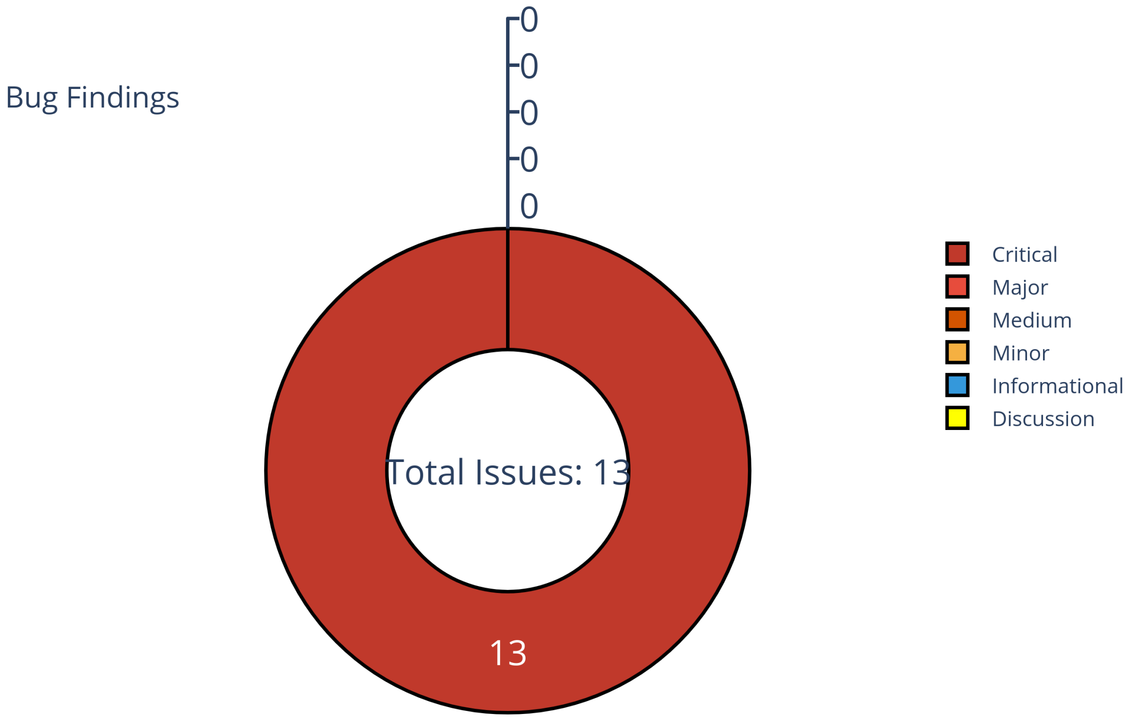

Figure 1: Findings

ID	Title	Category	Severity	Status
INT_CVE_0	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_1	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_2	Overflow	Integer Overflow wpa	Critical	UnResolved
INT_CVE_3	Overflow	Integer Overflow wpa	Critical	UnResolved

ID	Title	Category	Severity	Status
TYP_CVE_0	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_1	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_2	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_3	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_4	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_5	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_6	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_7	Instruction id not checked error	Instruction id issue	Critical	UnResolved
TYP_CVE_8	Instruction id not checked error	Instruction id issue	Critical	UnResolved

Issue: INT_CVE_0: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

level1/src/processor.rs:181:5: 181:50

```
181 **wallet_info.lamports.borrow_mut() -= amount
182
```

- Code Context

– Function Definition:

```
153 fn withdraw(program_id: &Pubkey, accounts: &[AccountInfo], amount: u64) -> ProgramResult
154
```

Vulnerability at Line: 181

```
176
177     if amount > **wallet_info.lamports.borrow_mut() {
178         return Err(ProgramError::InsufficientFunds);
179     }
180
181     **wallet_info.lamports.borrow_mut() -= amount;
182     **destination_info.lamports.borrow_mut() += amount;
183
184     wallet
185         .serialize(&mut &mut (*wallet_info.data).borrow_mut()[..])
186
```

- Call Stack

```
level1/src/processor.rs
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_1: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

level1/src/processor.rs:182:5: 182:55

```
182 **destination_info.lamports.borrow_mut() += amount
183
```

- Code Context

– Function Definition:

```
153 fn withdraw(program_id: &Pubkey, accounts: &[AccountInfo], amount: u64) -> ProgramResult
154
```

Vulnerability at Line: 182

```
177     if amount > **wallet_info.lamports.borrow_mut() {
178         return Err(ProgramError::InsufficientFunds);
179     }
180
181     **wallet_info.lamports.borrow_mut() -= amount;
182     **destination_info.lamports.borrow_mut() += amount;
183
184     wallet
185         .serialize(&mut &mut (*wallet_info.data).borrow_mut()[..])
186         .unwrap();
187
```

- Call Stack

```
1 level1/src/processor.rs
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_2: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.8.2/src/rent.rs:57:10:57:76

```
((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year)
```

- Code Context

Vulnerability at Line: 57

```
pub fn minimum_balance(&self, data_len: usize) -> u64 {
        let bytes = data_len as u64;
        (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
            * self.exemption_threshold) as u64
    }
```

- Call Stack

```
/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.8.2/src/rent.rs
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: INT_CVE_3: IntegerCve - Overflow

Category	Severity	Status
Integer Overflow wpa	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.8.2/src/rent.rs:57:9: 58:40

```
57  (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58              * self.exemption_threshold)
59
```

- Code Context

Vulnerability at Line: 57

```
55  pub fn minimum_balance(&self, data_len: usize) -> u64 {
56          let bytes = data_len as u64;
57          (((ACCOUNT_STORAGE_OVERHEAD + bytes) * self.lamports_per_byte_year) as f64
58              * self.exemption_threshold) as u64
59      }
60
```

- Call Stack

```
/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.8.2/src/rent.rs
```

- description:

Description of the bug here.

- link:

GitHub Link to be added.

- alleviation:

Some alleviation steps here.

Issue: TYP_CVE_0: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

level1/src/processor.rs:153:1: 189:2

```rust
fn withdraw(program_id: &Pubkey, accounts: &[AccountInfo], amount: u64) -> ProgramResult {
    msg!("withdraw {}", amount);
    let account_info_iter = &mut accounts.iter();
    let wallet_info = next_account_info(account_info_iter)?;
    let authority_info = next_account_info(account_info_iter)?;
    let destination_info = next_account_info(account_info_iter)?;
    let wallet = Wallet::deserialize(&mut &(*wallet_info.data).borrow_mut()[..])?;

    assert_eq!(wallet_info.owner, program_id);
    assert_eq!(wallet.authority, *authority_info.key);

    let res = check_assert(authority_info.is_signer);
    if res.is_ok(){
        msg!("check assert success.");
    }

    // if !authority_info.is_signer { // authority_info authority owner admin manager
    //     return  Err(ProgramError::InsufficientFunds);
    // }

    // Mitigation:
    // assert!(authority_info.is_signer);    // assert_eq!(authority_info.is_signer, true);
    // assert_eq!(authority_info.is_signer, true);

    if amount > **wallet_info.lamports.borrow_mut() {
        return Err(ProgramError::InsufficientFunds);
    }

    **wallet_info.lamports.borrow_mut() -= amount;
    **destination_info.lamports.borrow_mut() += amount;

    wallet
        .serialize(&mut &mut (*wallet_info.data).borrow_mut()[..])
        .unwrap();

    Ok(())
}

```

- Call Stack

```
fn entrypoint(){// /home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.8.2/src/entrypoint.rs:119:9: 126:10 }
    fn processor::process_instruction(){// level1/src/processor.rs:16:1: 26:2 }
        fn processor::withdraw(){// level1/src/processor.rs:153:1: 189:2 }

```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_1: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

level1/src/processor.rs:153:1: 189:2

```rust
fn withdraw(program_id: &Pubkey, accounts: &[AccountInfo], amount: u64) -> ProgramResult {
    msg!("withdraw {}", amount);
    let account_info_iter = &mut accounts.iter();
    let wallet_info = next_account_info(account_info_iter)?;
    let authority_info = next_account_info(account_info_iter)?;
    let destination_info = next_account_info(account_info_iter)?;
    let wallet = Wallet::deserialize(&mut &(*wallet_info.data).borrow_mut()[..])?;

    assert_eq!(wallet_info.owner, program_id);
    assert_eq!(wallet.authority, *authority_info.key);

    let res = check_assert(authority_info.is_signer);
    if res.is_ok(){
        msg!("check assert success.");
    }

    // if !authority_info.is_signer { // authority_info authority owner admin manager
    //     return  Err(ProgramError::InsufficientFunds);
    // }

    // Mitigation:
    // assert!(authority_info.is_signer);    // assert_eq!(authority_info.is_signer, true);
    // assert_eq!(authority_info.is_signer, true);

    if amount > **wallet_info.lamports.borrow_mut() {
        return Err(ProgramError::InsufficientFunds);
    }

    **wallet_info.lamports.borrow_mut() -= amount;
    **destination_info.lamports.borrow_mut() += amount;

    wallet
        .serialize(&mut &mut (*wallet_info.data).borrow_mut()[..])
        .unwrap();

    Ok(())
}

```

- Call Stack

```
fn entrypoint(){// /home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.8.2/src/entrypoint.rs:119:9: 126:10 }
    fn processor::process_instruction(){// level1/src/processor.rs:16:1: 26:2 }
        fn processor::withdraw(){// level1/src/processor.rs:153:1: 189:2 }

```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_2: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.8.2/src/account_info.rs:111:5: 115:6

```
pub fn try_borrow_mut_data(&self) -> Result<RefMut<&'a mut [u8]>, ProgramError> {
        self.data
            .try_borrow_mut()
            .map_err(|_| ProgramError::AccountBorrowFailed)
    }

```

- Call Stack

```
fn entrypoint(){// /home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.8.2/src/entrypoint.rs:119:9: 126:10 }
    fn processor::process_instruction(){// level1/src/processor.rs:16:1: 26:2 }
        fn processor::deposit(){// level1/src/processor.rs:137:1: 151:2 }
            fn solana_program::program::invoke(){// /home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.8.2/src/program.rs:12:1: 14:2 }
                fn solana_program::program::invoke_signed(){// /home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.8.2/src/program.rs:35:1: 57:2 }
                    fn solana_program::account_info::AccountInfo::<'a>::try_borrow_
                    /home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.8.2/src/account_info.rs:111:5: 115:6 }
```

```

```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_3: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.8.2/src/account_info.rs:105:5: 109:6

```
pub fn try_borrow_data(&self) -> Result<Ref<&mut [u8]>, ProgramError> {
        self.data
            .try_borrow()
            .map_err(|_| ProgramError::AccountBorrowFailed)
    }

```

- Call Stack

```
fn entrypoint(){// /home/ubuntu/.cargo/registry/src/github.com-
↪   1ecc6299db9ec823/solana-program-1.8.2/src/entrypoint.rs:119:9: 126:10
↪   }
    fn processor::process_instruction(){// level1/src/processor.rs:16:1:
    ↪   26:2 }
        fn processor::deposit(){// level1/src/processor.rs:137:1: 151:2 }
            fn solana_program::program::invoke(){//
            ↪   /home/ubuntu/.cargo/registry/src/github.com-
            ↪   1ecc6299db9ec823/solana-program-1.8.2/src/program.rs:12:1:
            ↪   14:2 }
                    fn solana_program::program::invoke_signed(){//
                    ↪   /home/ubuntu/.cargo/registry/src/github.com-
                    ↪   1ecc6299db9ec823/solana-program-
                    ↪   1.8.2/src/program.rs:35:1: 57:2
                    ↪   }
                        fn
                        ↪   solana_program::account_info::AccountInfo::<'a>::try_borrow_
                        ↪   /home/ubuntu/.cargo/registry/src/github.com-
                        ↪   1ecc6299db9ec823/solana-program-
                        ↪   1.8.2/src/account_info.rs:105:5: 109:6
                        ↪   }
```

```

```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_4: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.8.2/src/sysvar/mod.rs:70:5: 75:6

```
fn from_account_info(account_info: &AccountInfo) -> Result<Self,
↪   ProgramError> {
        if !Self::check_id(account_info.unsigned_key()) {
            return Err(ProgramError::InvalidArgument);
        }
        bincode::deserialize(&account_info.data.borrow()).map_err(|_|
        ↪   ProgramError::InvalidArgument)
    }

```

- Call Stack

```
fn entrypoint(){// /home/ubuntu/.cargo/registry/src/github.com-
↪   1ecc6299db9ec823/solana-program-1.8.2/src/entrypoint.rs:119:9: 126:10
↪   }
    fn processor::process_instruction(){// level1/src/processor.rs:16:1:
    ↪   26:2 }
        fn processor::initialize(){// level1/src/processor.rs:28:1: 63:2 }
            fn solana_program::sysvar::Sysvar::from_account_info(){//
            ↪   /home/ubuntu/.cargo/registry/src/github.com-
            ↪   1ecc6299db9ec823/solana-program-
            ↪   1.8.2/src/sysvar/mod.rs:70:5: 75:6
            ↪   }

```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_5: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.8.2/src/account_info.rs:85:5: 87:6

```rust
pub fn data_is_empty(&self) -> bool {
        self.data.borrow().is_empty()
    }

```

- Call Stack

```rust
fn entrypoint(){// /home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.8.2/src/entrypoint.rs:119:9: 126:10 }
    fn processor::process_instruction(){// level1/src/processor.rs:16:1: 26:2 }
        fn processor::initialize(){// level1/src/processor.rs:28:1: 63:2 }
            fn solana_program::account_info::AccountInfo::<'a>::data_is_empty(){// /home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.8.2/src/account_info.rs:85:5: 87:6 }

```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_6: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.8.2/src/account_info.rs:111:5: 115:6

```
pub fn try_borrow_mut_data(&self) -> Result<RefMut<&'a mut [u8]>, ProgramError> {
        self.data
            .try_borrow_mut()
            .map_err(|_| ProgramError::AccountBorrowFailed)
    }

```

- Call Stack

```
fn entrypoint(){// /home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.8.2/src/entrypoint.rs:119:9: 126:10 }
    fn processor::process_instruction(){// level1/src/processor.rs:16:1: 26:2 }
        fn processor::initialize(){// level1/src/processor.rs:28:1: 63:2 }
            fn solana_program::program::invoke_signed(){// /home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.8.2/src/program.rs:35:1: 57:2 }
                fn solana_program::account_info::AccountInfo::<'a>::try_borrow_mut_
                /home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.8.2/src/account_info.rs:111:5: 115:6 }

```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_7: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

/home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.8.2/src/account_info.rs:105:5: 109:6

```
pub fn try_borrow_data(&self) -> Result<Ref<&mut [u8]>, ProgramError> {
        self.data
            .try_borrow()
            .map_err(|_| ProgramError::AccountBorrowFailed)
    }

```

- Call Stack

```
fn entrypoint(){// /home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.8.2/src/entrypoint.rs:119:9: 126:10 }
    fn processor::process_instruction(){// level1/src/processor.rs:16:1: 26:2 }
        fn processor::initialize(){// level1/src/processor.rs:28:1: 63:2 }
            fn solana_program::program::invoke_signed(){// /home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.8.2/src/program.rs:35:1: 57:2 }
                fn solana_program::account_info::AccountInfo::<'a>::try_borrow_data /home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.8.2/src/account_info.rs:105:5: 109:6 }

```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

Issue: TYP_CVE_8: InstructionId - Instruction id not checked error

Category	Severity	Status
Instruction id issue	Critical	UnResolved

- Location

level1/src/processor.rs:28:1: 63:2

```rust
fn initialize(program_id: &Pubkey, accounts: &[AccountInfo]) -> ProgramResult {
    msg!("init");
    let account_info_iter = &mut accounts.iter();
    let wallet_info = next_account_info(account_info_iter)?;
    let authority = next_account_info(account_info_iter)?;
    let rent_info = next_account_info(account_info_iter)?;
    let (wallet_address, wallet_seed) =
        Pubkey::find_program_address(&[&authority.key.to_bytes()], program_id);
    let rent = Rent::from_account_info(rent_info)?;

    assert_eq!(*wallet_info.key, wallet_address);
    assert!(wallet_info.data_is_empty());
    assert!(authority.is_signer, "authority must sign!");

    invoke_signed(
        &system_instruction::create_account(
            &authority.key,
            &wallet_address,
            rent.minimum_balance(WALLET_LEN as usize),
            WALLET_LEN,
            &program_id,
        ),
        &[authority.clone(), wallet_info.clone()],
        &[&[&authority.key.to_bytes(), &[wallet_seed]]],
    )?;

    let wallet = Wallet {
        authority: *authority.key,
    };

    wallet
        .serialize(&mut &mut (*wallet_info.data).borrow_mut()[..])
        .unwrap();

    Ok(())
}

```

- Call Stack

```
fn entrypoint(){// /home/ubuntu/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.8.2/src/entrypoint.rs:119:9: 126:10 }
    fn processor::process_instruction(){// level1/src/processor.rs:16:1: 26:2 }
        fn processor::initialize(){// level1/src/processor.rs:28:1: 63:2 }

```

- description:

message

- link:

GitHub Link to be added.

- alleviation:

Description of the bug here.

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.