VRust

Security Assessment

O2Lab VRust Team

11/02/2022 20:55:15

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

Audit Summary

Delivery Date	11/02/2022
Audit Methodology	Static Analysis
Key Components	

Vulnerability Summary

Vulnerability Level	Total
Critical	10
Major	0
Medium	0
Minor	0
Informational	0
Discussion	0

Findings

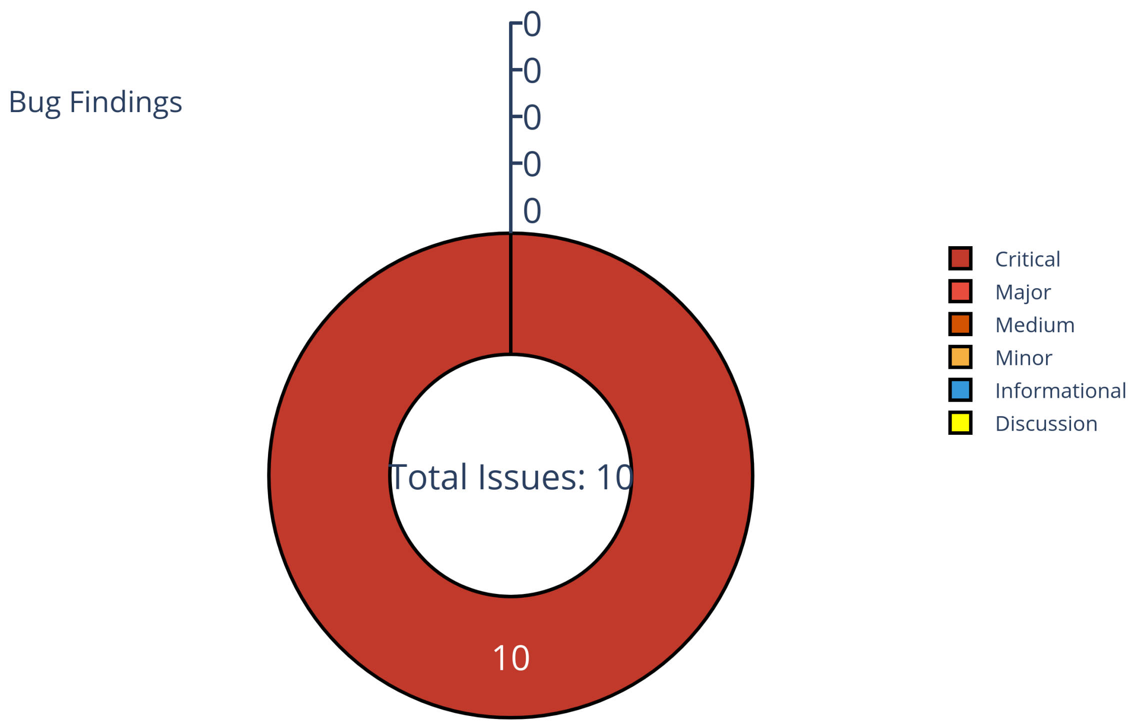

Figure 1: Findings

Finding Statistic

Category	Count
IntegerFlow	1
MissingKeyCheck	1
CrossProgramInvocation	8

ID	Category	Severity	Status
0	IntegerFlow	Critical	UnResolved
1	MissingKeyCheck	Critical	UnResolved
2	CrossProgramInvocation	Critical	UnResolved
3	CrossProgramInvocation	Critical	UnResolved
4	CrossProgramInvocation	Critical	UnResolved
5	CrossProgramInvocation	Critical	UnResolved
6	CrossProgramInvocation	Critical	UnResolved
7	CrossProgramInvocation	Critical	UnResolved
8	CrossProgramInvocation	Critical	UnResolved
9	CrossProgramInvocation	Critical	UnResolved

Issue: 0: IntegerFlow

Category	Severity	Status
IntegerFlow	Critical	UnResolved

- Location

program/src/api/transfer.rs:174:23: 174:50

```
174 data.amount / trunc_divisor
175
```

- Code Context

Vulnerability at Line: 174

```
169         invoke_signed(&init_ix, ctx.accounts, &[])?;
170     }
171
172     let trunc_divisor = 10u64.pow(8.max(accs.mint.decimals as u32) - 8);
173     // Truncate to 8 decimals
174     let amount: u64 = data.amount / trunc_divisor;
175     let fee: u64 = data.fee / trunc_divisor;
176     // Untruncate the amount to drop the remainder so we don't  "burn"
        ↪  user's funds.
177     let amount_trunc: u64 = amount * trunc_divisor;
178
179
```

- Call Stack

```
1 fn entrypoint(){// /home/yifei/.cargo/registry/src/github.com-
  ↪  1ecc6299db9ec823/solana-program-1.7.0/src/entrypoint.rs:46:9: 53:10
  ↪  }
2     fn instruction::solitaire(){//
      ↪  /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/macros.rs
      ↪  108:14 }
3         fn instruction::dispatch(){//
          ↪  /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/macro
          ↪  99:14 }
```

```
            fn instruction::TransferNative::execute(){//
            ↪  /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/m
            ↪  74:22 }
                    fn api::transfer::transfer_native(){//
                    ↪  program/src/api/transfer.rs:127:1: 234:2 }

```

- description:
- link:
- alleviation:

Issue: 1: MissingKeyCheck

Category	Severity	Status
MissingKeyCheck	Critical	UnResolved

- Location

/home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/processors/peel.rs:211:22:211:50

```
211 ctx.info().lamports.borrow()
212
```

- Code Context

– Function Definition:

```
192 fn peel<I>(ctx: &'c mut Context<'a, 'b, 'c, I>) -> Result<Self>
193
```

Vulnerability at Line: 202

```
197         }
198
199         // If we're initializing the type, we should emit system/rent as
             ↪  deps.
200         let (initialized, data): (bool, T) = match IsInitialized {
201             AccountState::Uninitialized => {
202                 if **ctx.info().lamports.borrow() != 0 {
203                     return
                         ↪  Err(SolitaireError::AlreadyInitialized(*ctx.info().key));
204                 }
205                 (false, T::default())
206             }
207
```

Other Use Case for Variable: ctx.info().lamports.borrow()

```
            if **ctx.info().lamports.borrow() == 0 {
```

- Call Stack

```
fn entrypoint(){// /home/yifei/.cargo/registry/src/github.com-
↪   1ecc6299db9ec823/solana-program-1.7.0/src/entrypoint.rs:46:9: 53:10
↪   }
    fn instruction::solitaire(){//
    ↪   /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/macros.rs
    ↪   108:14 }
        fn instruction::dispatch(){//
        ↪   /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/macro
        ↪   99:14 }
            fn instruction::AttestToken::execute(){//
            ↪   /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/m
            ↪   74:22 }
                    fn <api::attest::AttestToken<'b> as
                    ↪   solitaire::FromAccounts<'a, 'b, 'c>>::from(){//
                    ↪   program/src/api/attest.rs:68:10: 68:22 }
                        fn <solitaire::Data<'b, T, IsInitialized> as
                        ↪   solitaire::Peel<'a, 'b, 'c>>::peel(){//
                        ↪   /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/p
                        ↪   236:6 }
```

- description:
- link:
- alleviation:

Issue: 2: CrossProgramInvocation

Category	Severity	Status
CrossProgramInvocation	Critical	UnResolved

- Location

```
program/src/api/complete_transfer.rs
```

- Code Context

```rust
pub fn complete_native(
    ctx: &ExecutionContext,
    accs: &mut CompleteNative,
    data: CompleteNativeData,
) -> Result<()> {
    // Verify the chain registration
    let derivation_data: EndpointDerivationData = (&*accs).into();
    accs.chain_registration
        .verify_derivation(ctx.program_id, &derivation_data)?;

    // Verify that the custody account is derived correctly
    let derivation_data: CustodyAccountDerivationData = (&*accs).into();
    accs.custody
        .verify_derivation(ctx.program_id, &derivation_data)?;

    // Verify mints
    if *accs.mint.info().key != accs.to.mint {
        return Err(InvalidMint.into());
    }
    if *accs.mint.info().key != accs.to_fees.mint {
        return Err(InvalidMint.into());
    }
    if *accs.mint.info().key != accs.custody.mint {
        return Err(InvalidMint.into());
    }
    if *accs.custody_signer.key != accs.custody.owner {
        return Err(WrongAccountOwner.into());
    }

    // Verify VAA
    if accs.vaa.token_address != accs.mint.info().key.to_bytes() {
        return Err(InvalidMint.into());
    }
    if accs.vaa.token_chain != 1 {
        return Err(InvalidChain.into());
    }
    if accs.vaa.to_chain != CHAIN_ID_SOLANA {
        return Err(InvalidChain.into());
    }
    if accs.vaa.to != accs.to.info().key.to_bytes() {
        return Err(InvalidRecipient.into());
    }

    // Prevent vaa double signing
    accs.vaa.verify(ctx.program_id)?;
    accs.vaa.claim(ctx, accs.payer.key)?;

    let mut amount = accs.vaa.amount.as_u64();
    let mut fee = accs.vaa.fee.as_u64();

    // Wormhole always caps transfers at 8 decimals; un-truncate if the
     ↪ local token has more
    if accs.mint.decimals > 8 {
        amount *= 10u64.pow((accs.mint.decimals - 8) as u32);
        fee *= 10u64.pow((accs.mint.decimals - 8) as u32);
    }

    // Transfer tokens
    let transfer_ix = spl_token::instruction::transfer(
        &spl_token::id(),
        accs.custody.info().key,
        accs.to.info().key,
        accs.custody_signer.key,
        &[],
        amount.checked_sub(fee).unwrap(),
    )?;
    invoke_seeded(&transfer_ix, ctx, &accs.custody_signer, None)?;

    // Transfer fees
    let transfer_ix = spl_token::instruction::transfer(
        &spl_token::id(),
        accs.custody.info().key,
        accs.to_fees.info().key,
        accs.custody_signer.key,
        &[],
        fee,
    )?;
    invoke_seeded(&transfer_ix, ctx, &accs.custody_signer, None)?;

    Ok(())
}

```

- Call Stack

```
fn entrypoint(){// /home/yifei/.cargo/registry/src/github.com-
↪   1ecc6299db9ec823/solana-program-1.7.0/src/entrypoint.rs:46:9: 53:10
↪   }
    fn instruction::solitaire(){//
    ↪   /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/macros.rs
    ↪   108:14 }
        fn instruction::dispatch(){//
        ↪   /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/macro
        ↪   99:14 }
            fn instruction::CompleteNative::execute(){//
            ↪   /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/m
            ↪   74:22 }
                fn api::complete_transfer::complete_native(){//
                ↪   program/src/api/complete_transfer.rs:85:1: 164:2 }

```

- description:
- link:
- alleviation:

Issue: 3: CrossProgramInvocation

Category	Severity	Status
CrossProgramInvocation	Critical	UnResolved

- Location

```
program/src/api/complete_transfer.rs
```

- Code Context

```rust
pub fn complete_native(
    ctx: &ExecutionContext,
    accs: &mut CompleteNative,
    data: CompleteNativeData,
) -> Result<()> {
    // Verify the chain registration
    let derivation_data: EndpointDerivationData = (&*accs).into();
    accs.chain_registration
        .verify_derivation(ctx.program_id, &derivation_data)?;

    // Verify that the custody account is derived correctly
    let derivation_data: CustodyAccountDerivationData = (&*accs).into();
    accs.custody
        .verify_derivation(ctx.program_id, &derivation_data)?;

    // Verify mints
    if *accs.mint.info().key != accs.to.mint {
        return Err(InvalidMint.into());
    }
    if *accs.mint.info().key != accs.to_fees.mint {
        return Err(InvalidMint.into());
    }
    if *accs.mint.info().key != accs.custody.mint {
        return Err(InvalidMint.into());
    }
    if *accs.custody_signer.key != accs.custody.owner {
        return Err(WrongAccountOwner.into());
    }

    // Verify VAA
    if accs.vaa.token_address != accs.mint.info().key.to_bytes() {
        return Err(InvalidMint.into());
    }
    if accs.vaa.token_chain != 1 {
        return Err(InvalidChain.into());
    }
    if accs.vaa.to_chain != CHAIN_ID_SOLANA {
        return Err(InvalidChain.into());
    }
    if accs.vaa.to != accs.to.info().key.to_bytes() {
        return Err(InvalidRecipient.into());
    }

    // Prevent vaa double signing
    accs.vaa.verify(ctx.program_id)?;
    accs.vaa.claim(ctx, accs.payer.key)?;

    let mut amount = accs.vaa.amount.as_u64();
    let mut fee = accs.vaa.fee.as_u64();

    // Wormhole always caps transfers at 8 decimals; un-truncate if the
     ↪  local token has more
    if accs.mint.decimals > 8 {
        amount *= 10u64.pow((accs.mint.decimals - 8) as u32);
        fee *= 10u64.pow((accs.mint.decimals - 8) as u32);
    }

    // Transfer tokens
    let transfer_ix = spl_token::instruction::transfer(
        &spl_token::id(),
        accs.custody.info().key,
        accs.to.info().key,
        accs.custody_signer.key,
        &[],
        amount.checked_sub(fee).unwrap(),
    )?;
    invoke_seeded(&transfer_ix, ctx, &accs.custody_signer, None)?;

    // Transfer fees
    let transfer_ix = spl_token::instruction::transfer(
        &spl_token::id(),
        accs.custody.info().key,
        accs.to_fees.info().key,
        accs.custody_signer.key,
        &[],
        fee,
    )?;
    invoke_seeded(&transfer_ix, ctx, &accs.custody_signer, None)?;

    Ok(())
}

```

- Call Stack

```
fn entrypoint(){// /home/yifei/.cargo/registry/src/github.com-
↪   1ecc6299db9ec823/solana-program-1.7.0/src/entrypoint.rs:46:9: 53:10
↪   }
    fn instruction::solitaire(){//
    ↪   /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/macros.rs
    ↪   108:14 }
        fn instruction::dispatch(){//
        ↪   /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/macro
        ↪   99:14 }
            fn instruction::CompleteNative::execute(){//
            ↪   /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/m
            ↪   74:22 }
                fn api::complete_transfer::complete_native(){//
                ↪   program/src/api/complete_transfer.rs:85:1: 164:2 }

```

- description:
- link:
- alleviation:

Issue: 4: CrossProgramInvocation

Category	Severity	Status
CrossProgramInvocation	Critical	UnResolved

- Location

```
program/src/api/complete_transfer.rs
```

- Code Context

```rust
pub fn complete_wrapped(
    ctx: &ExecutionContext,
    accs: &mut CompleteWrapped,
    data: CompleteWrappedData,
) -> Result<()> {
    // Verify the chain registration
    let derivation_data: EndpointDerivationData = (&*accs).into();
    accs.chain_registration
        .verify_derivation(ctx.program_id, &derivation_data)?;

    // Verify mint
    accs.wrapped_meta.verify_derivation(
        ctx.program_id,
        &WrappedMetaDerivationData {
            mint_key: *accs.mint.info().key,
        },
    )?;
    if accs.wrapped_meta.token_address != accs.vaa.token_address
        || accs.wrapped_meta.chain != accs.vaa.token_chain
    {
        return Err(InvalidMint.into());
    }

    // Verify mints
    if *accs.mint.info().key != accs.to.mint {
        return Err(InvalidMint.into());
    }
    if *accs.mint.info().key != accs.to_fees.mint {
        return Err(InvalidMint.into());
    }

    // Verify VAA
    if accs.vaa.to_chain != CHAIN_ID_SOLANA {
        return Err(InvalidChain.into());
    }
    if accs.vaa.to != accs.to.info().key.to_bytes() {
        return Err(InvalidRecipient.into());
    }

    accs.vaa.verify(ctx.program_id)?;
    accs.vaa.claim(ctx, accs.payer.key)?;

    // Mint tokens
    let mint_ix = spl_token::instruction::mint_to(
        &spl_token::id(),
        accs.mint.info().key,
        accs.to.info().key,
        accs.mint_authority.key,
        &[],
        accs.vaa
            .amount
            .as_u64()
            .checked_sub(accs.vaa.fee.as_u64())
            .unwrap(),
    )?;
    invoke_seeded(&mint_ix, ctx, &accs.mint_authority, None)?;

    // Mint fees
    let mint_ix = spl_token::instruction::mint_to(
        &spl_token::id(),
        accs.mint.info().key,
        accs.to_fees.info().key,
        accs.mint_authority.key,
        &[],
        accs.vaa.fee.as_u64(),
    )?;
    invoke_seeded(&mint_ix, ctx, &accs.mint_authority, None)?;

    Ok(())
```

```
}

```

- Call Stack

```
fn entrypoint(){// /home/yifei/.cargo/registry/src/github.com-
↪  1ecc6299db9ec823/solana-program-1.7.0/src/entrypoint.rs:46:9: 53:10
↪  }
    fn instruction::solitaire(){//
    ↪  /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/macros.rs
    ↪  108:14 }
        fn instruction::dispatch(){//
        ↪  /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/macro
        ↪  99:14 }
            fn instruction::CompleteWrapped::execute(){//
            ↪  /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/m
            ↪  74:22 }
                fn api::complete_transfer::complete_wrapped(){//
                ↪  program/src/api/complete_transfer.rs:208:1: 277:2 }

```

- description:
- link:
- alleviation:

Issue: 5: CrossProgramInvocation

Category	Severity	Status
CrossProgramInvocation	Critical	UnResolved

- Location

```
program/src/api/complete_transfer.rs
```

- Code Context

```rust
pub fn complete_wrapped(
    ctx: &ExecutionContext,
    accs: &mut CompleteWrapped,
    data: CompleteWrappedData,
) -> Result<()> {
    // Verify the chain registration
    let derivation_data: EndpointDerivationData = (&*accs).into();
    accs.chain_registration
        .verify_derivation(ctx.program_id, &derivation_data)?;

    // Verify mint
    accs.wrapped_meta.verify_derivation(
        ctx.program_id,
        &WrappedMetaDerivationData {
            mint_key: *accs.mint.info().key,
        },
    )?;
    if accs.wrapped_meta.token_address != accs.vaa.token_address
        || accs.wrapped_meta.chain != accs.vaa.token_chain
    {
        return Err(InvalidMint.into());
    }

    // Verify mints
    if *accs.mint.info().key != accs.to.mint {
        return Err(InvalidMint.into());
    }
    if *accs.mint.info().key != accs.to_fees.mint {
        return Err(InvalidMint.into());
    }

    // Verify VAA
    if accs.vaa.to_chain != CHAIN_ID_SOLANA {
        return Err(InvalidChain.into());
    }
    if accs.vaa.to != accs.to.info().key.to_bytes() {
        return Err(InvalidRecipient.into());
    }

    accs.vaa.verify(ctx.program_id)?;
    accs.vaa.claim(ctx, accs.payer.key)?;

    // Mint tokens
    let mint_ix = spl_token::instruction::mint_to(
        &spl_token::id(),
        accs.mint.info().key,
        accs.to.info().key,
        accs.mint_authority.key,
        &[],
        accs.vaa
            .amount
            .as_u64()
            .checked_sub(accs.vaa.fee.as_u64())
            .unwrap(),
    )?;
    invoke_seeded(&mint_ix, ctx, &accs.mint_authority, None)?;

    // Mint fees
    let mint_ix = spl_token::instruction::mint_to(
        &spl_token::id(),
        accs.mint.info().key,
        accs.to_fees.info().key,
        accs.mint_authority.key,
        &[],
        accs.vaa.fee.as_u64(),
    )?;
    invoke_seeded(&mint_ix, ctx, &accs.mint_authority, None)?;

    Ok(())
```

```
}

```

- Call Stack

```
fn entrypoint(){// /home/yifei/.cargo/registry/src/github.com-
↪  1ecc6299db9ec823/solana-program-1.7.0/src/entrypoint.rs:46:9: 53:10
↪  }
    fn instruction::solitaire(){//
    ↪  /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/macros.rs
    ↪  108:14 }
        fn instruction::dispatch(){//
        ↪  /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/macro
        ↪  99:14 }
            fn instruction::CompleteWrapped::execute(){//
            ↪  /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/m
            ↪  74:22 }
                    fn api::complete_transfer::complete_wrapped(){//
                    ↪  program/src/api/complete_transfer.rs:208:1: 277:2 }

```

- description:
- link:
- alleviation:

Issue: 6: CrossProgramInvocation

Category	Severity	Status
CrossProgramInvocation	Critical	UnResolved

- Location

```
program/src/api/transfer.rs
```

- Code Context

```
pub fn transfer_wrapped(
    ctx: &ExecutionContext,
    accs: &mut TransferWrapped,
    data: TransferWrappedData,
) -> Result<()> {
    // Prevent transferring to the same chain.
    if data.target_chain == CHAIN_ID_SOLANA {
        return Err(InvalidChain.into());
    }

    // Verify that the from account is owned by the from_owner
    if &accs.from.owner != accs.from_owner.key {
        return Err(WrongAccountOwner.into());
    }

    // Verify mints
    if accs.mint.info().key != &accs.from.mint {
        return Err(TokenBridgeError::InvalidMint.into());
    }

    // Fee must be less than amount
    if data.fee > data.amount {
        return Err(InvalidFee.into());
    }

    // Verify that meta is correct
    let derivation_data: WrappedMetaDerivationData = (&*accs).into();
    accs.wrapped_meta
        .verify_derivation(ctx.program_id, &derivation_data)?;

    // Burn tokens
    let burn_ix = spl_token::instruction::burn(
        &spl_token::id(),
        accs.from.info().key,
        accs.mint.info().key,
        accs.authority_signer.key,
        &[],
        data.amount,
    )?;
    invoke_seeded(&burn_ix, ctx, &accs.authority_signer, None)?;

    // Pay fee
    let transfer_ix = solana_program::system_instruction::transfer(
        accs.payer.key,
        accs.fee_collector.key,
        accs.bridge.config.fee,
    );

    invoke(&transfer_ix, ctx.accounts)?;

    // Post message
    let payload = PayloadTransfer {
        amount: U256::from(data.amount),
        token_address: accs.wrapped_meta.token_address,
        token_chain: accs.wrapped_meta.chain,
        to: data.target_address,
        to_chain: data.target_chain,
        fee: U256::from(data.fee),
    };
    let params = (
        bridge::instruction::Instruction::PostMessage,
        PostMessageData {
            nonce: data.nonce,
            payload: payload.try_to_vec()?,
            consistency_level: ConsistencyLevel::Finalized,
        },
    );

    let ix = Instruction::new_with_bytes(
        accs.config.wormhole_bridge,
        params.try_to_vec()?.as_slice(),
        vec![
            AccountMeta::new(*accs.bridge.info().key, false),
            AccountMeta::new(*accs.message.key, true),
            AccountMeta::new_readonly(*accs.emitter.key, true),
            AccountMeta::new(*accs.sequence.key, false),
            AccountMeta::new(*accs.payer.key, true),
            AccountMeta::new(*accs.fee_collector.key, false),
            AccountMeta::new_readonly(*accs.clock.info().key, false),
            AccountMeta::new_readonly(solana_program::system_program::id(),
            ↪   false),
            AccountMeta::new_readonly(solana_program::sysvar::rent::ID,
            ↪   false),
        ],
    );
    invoke_seeded(&ix, ctx, &accs.emitter, None)?;

    Ok(())
}

```

- Call Stack

```
fn entrypoint(){// /home/yifei/.cargo/registry/src/github.com-
↪   1ecc6299db9ec823/solana-program-1.7.0/src/entrypoint.rs:46:9: 53:10
↪   }
    fn instruction::solitaire(){//
    ↪   /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/macros.rs
    ↪   108:14 }
        fn instruction::dispatch(){//
        ↪   /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/macro
        ↪   99:14 }
            fn instruction::TransferWrapped::execute(){//
            ↪   /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/m
            ↪   74:22 }
                fn api::transfer::transfer_wrapped(){//
                ↪   program/src/api/transfer.rs:295:1: 381:2 }

```

- description:

- link:
- alleviation:

Issue: 7: CrossProgramInvocation

Category	Severity	Status
CrossProgramInvocation	Critical	UnResolved

- Location

```
program/src/api/transfer.rs
```

- Code Context

```rust
pub fn transfer_native(
    ctx: &ExecutionContext,
    accs: &mut TransferNative,
    data: TransferNativeData,
) -> Result<()> {
    // Prevent transferring to the same chain.
    if data.target_chain == CHAIN_ID_SOLANA {
        return Err(InvalidChain.into());
    }

    // Verify that the custody account is derived correctly
    let derivation_data: CustodyAccountDerivationData = (&*accs).into();
    accs.custody
        .verify_derivation(ctx.program_id, &derivation_data)?;

    // Verify mints
    if accs.from.mint != *accs.mint.info().key {
        return Err(TokenBridgeError::InvalidMint.into());
    }

    // Fee must be less than amount
    if data.fee > data.amount {
        return Err(InvalidFee.into());
    }

    // Verify that the token is not a wrapped token
    if let COption::Some(mint_authority) = accs.mint.mint_authority {
        if mint_authority == MintSigner::key(None, ctx.program_id) {
            return Err(TokenBridgeError::TokenNotNative.into());
        }
    }

    if !accs.custody.is_initialized() {
        accs.custody
            .create(&(&*accs).into(), ctx, accs.payer.key, Exempt)?;

        let init_ix = spl_token::instruction::initialize_account(
            &spl_token::id(),
            accs.custody.info().key,
            accs.mint.info().key,
            accs.custody_signer.key,
        )?;
        invoke_signed(&init_ix, ctx.accounts, &[])?;
    }

    let trunc_divisor = 10u64.pow(8.max(accs.mint.decimals as u32) - 8);
    // Truncate to 8 decimals
    let amount: u64 = data.amount / trunc_divisor;
    let fee: u64 = data.fee / trunc_divisor;
    // Untruncate the amount to drop the remainder so we don't  "burn"
    ↪  user's funds.
    let amount_trunc: u64 = amount * trunc_divisor;

    // Transfer tokens
    let transfer_ix = spl_token::instruction::transfer(
        &spl_token::id(),
        accs.from.info().key,
        accs.custody.info().key,
        accs.authority_signer.key,
        &[],
        amount_trunc,
    )?;
    invoke_seeded(&transfer_ix, ctx, &accs.authority_signer, None)?;

    // Pay fee
    let transfer_ix = solana_program::system_instruction::transfer(
        accs.payer.key,
        accs.fee_collector.key,
        accs.bridge.config.fee,
    );
    invoke(&transfer_ix, ctx.accounts)?;

    // Post message
    let payload = PayloadTransfer {
        amount: U256::from(amount),
        token_address: accs.mint.info().key.to_bytes(),
        token_chain: CHAIN_ID_SOLANA,
        to: data.target_address,
        to_chain: data.target_chain,
        fee: U256::from(fee),
    };
    let params = (
        bridge::instruction::Instruction::PostMessage,
        PostMessageData {
            nonce: data.nonce,
            payload: payload.try_to_vec()?,
            consistency_level: ConsistencyLevel::Finalized,
        },
    );

    let ix = Instruction::new_with_bytes(
        accs.config.wormhole_bridge,
        params.try_to_vec()?.as_slice(),
        vec![
            AccountMeta::new(*accs.bridge.info().key, false),
            AccountMeta::new(*accs.message.key, true),
            AccountMeta::new_readonly(*accs.emitter.key, true),
            AccountMeta::new(*accs.sequence.key, false),
            AccountMeta::new(*accs.payer.key, true),
            AccountMeta::new(*accs.fee_collector.key, false),
            AccountMeta::new_readonly(*accs.clock.info().key, false),
            AccountMeta::new_readonly(solana_program::system_program::id(),
             ↪  false),
            AccountMeta::new_readonly(solana_program::sysvar::rent::ID,
             ↪  false),
        ],
    );
    invoke_seeded(&ix, ctx, &accs.emitter, None)?;

    Ok(())
}
```

```
235
```

- Call Stack

```
fn entrypoint(){// /home/yifei/.cargo/registry/src/github.com-
↪  1ecc6299db9ec823/solana-program-1.7.0/src/entrypoint.rs:46:9: 53:10
↪  }
    fn instruction::solitaire(){//
    ↪  /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/macros.rs
    ↪  108:14 }
        fn instruction::dispatch(){//
        ↪  /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/macro
        ↪  99:14 }
            fn instruction::TransferNative::execute(){//
            ↪  /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/m
            ↪  74:22 }
                fn api::transfer::transfer_native(){//
                ↪  program/src/api/transfer.rs:127:1: 234:2 }
```

- description:
- link:
- alleviation:

Issue: 8: CrossProgramInvocation

Category	Severity	Status
CrossProgramInvocation	Critical	UnResolved

- Location

```
program/src/api/transfer.rs
```

- Code Context

```rust
pub fn transfer_native(
    ctx: &ExecutionContext,
    accs: &mut TransferNative,
    data: TransferNativeData,
) -> Result<()> {
    // Prevent transferring to the same chain.
    if data.target_chain == CHAIN_ID_SOLANA {
        return Err(InvalidChain.into());
    }

    // Verify that the custody account is derived correctly
    let derivation_data: CustodyAccountDerivationData = (&*accs).into();
    accs.custody
        .verify_derivation(ctx.program_id, &derivation_data)?;

    // Verify mints
    if accs.from.mint != *accs.mint.info().key {
        return Err(TokenBridgeError::InvalidMint.into());
    }

    // Fee must be less than amount
    if data.fee > data.amount {
        return Err(InvalidFee.into());
    }

    // Verify that the token is not a wrapped token
    if let COption::Some(mint_authority) = accs.mint.mint_authority {
        if mint_authority == MintSigner::key(None, ctx.program_id) {
            return Err(TokenBridgeError::TokenNotNative.into());
        }
    }

    if !accs.custody.is_initialized() {
        accs.custody
            .create(&(&*accs).into(), ctx, accs.payer.key, Exempt)?;

        let init_ix = spl_token::instruction::initialize_account(
            &spl_token::id(),
            accs.custody.info().key,
            accs.mint.info().key,
            accs.custody_signer.key,
        )?;
        invoke_signed(&init_ix, ctx.accounts, &[])?;
    }

    let trunc_divisor = 10u64.pow(8.max(accs.mint.decimals as u32) - 8);
    // Truncate to 8 decimals
    let amount: u64 = data.amount / trunc_divisor;
    let fee: u64 = data.fee / trunc_divisor;
    // Untruncate the amount to drop the remainder so we don't  "burn"
    ↪  user's funds.
    let amount_trunc: u64 = amount * trunc_divisor;

    // Transfer tokens
    let transfer_ix = spl_token::instruction::transfer(
        &spl_token::id(),
        accs.from.info().key,
        accs.custody.info().key,
        accs.authority_signer.key,
        &[],
        amount_trunc,
    )?;
    invoke_seeded(&transfer_ix, ctx, &accs.authority_signer, None)?;

    // Pay fee
    let transfer_ix = solana_program::system_instruction::transfer(
        accs.payer.key,
        accs.fee_collector.key,
        accs.bridge.config.fee,
    );
    invoke(&transfer_ix, ctx.accounts)?;

    // Post message
    let payload = PayloadTransfer {
        amount: U256::from(amount),
        token_address: accs.mint.info().key.to_bytes(),
        token_chain: CHAIN_ID_SOLANA,
        to: data.target_address,
        to_chain: data.target_chain,
        fee: U256::from(fee),
    };
    let params = (
        bridge::instruction::Instruction::PostMessage,
        PostMessageData {
            nonce: data.nonce,
            payload: payload.try_to_vec()?,
            consistency_level: ConsistencyLevel::Finalized,
        },
    );

    let ix = Instruction::new_with_bytes(
        accs.config.wormhole_bridge,
        params.try_to_vec()?.as_slice(),
        vec![
            AccountMeta::new(*accs.bridge.info().key, false),
            AccountMeta::new(*accs.message.key, true),
            AccountMeta::new_readonly(*accs.emitter.key, true),
            AccountMeta::new(*accs.sequence.key, false),
            AccountMeta::new(*accs.payer.key, true),
            AccountMeta::new(*accs.fee_collector.key, false),
            AccountMeta::new_readonly(*accs.clock.info().key, false),
            AccountMeta::new_readonly(solana_program::system_program::id(),
             ↪  false),
            AccountMeta::new_readonly(solana_program::sysvar::rent::ID,
             ↪  false),
        ],
    );
    invoke_seeded(&ix, ctx, &accs.emitter, None)?;

    Ok(())
}
```

- Call Stack

```
fn entrypoint(){// /home/yifei/.cargo/registry/src/github.com-1ecc6299db9ec823/solana-program-1.7.0/src/entrypoint.rs:46:9: 53:10 }
    fn instruction::solitaire(){// /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/macros.rs
    108:14 }
        fn instruction::dispatch(){// /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/macro
        99:14 }
            fn instruction::TransferNative::execute(){// /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/m
            74:22 }
                fn api::transfer::transfer_native(){// program/src/api/transfer.rs:127:1: 234:2 }

```

- description:
- link:
- alleviation:

Issue: 9: CrossProgramInvocation

Category	Severity	Status
CrossProgramInvocation	Critical	UnResolved

- Location

```
program/src/api/create_wrapped.rs
```

- Code Context

```rust
pub fn create_accounts(
    ctx: &ExecutionContext,
    accs: &mut CreateWrapped,
    data: CreateWrappedData,
) -> Result<()> {
    // Create mint account
    accs.mint
        .create(&((&*accs).into()), ctx, accs.payer.key, Exempt)?;

    // Initialize mint
    let init_ix = spl_token::instruction::initialize_mint(
        &spl_token::id(),
        accs.mint.info().key,
        accs.mint_authority.key,
        None,
        min(8, accs.vaa.decimals), // Limit to 8 decimals, truncation is
↪   handled on the other side
    )?;
    invoke_signed(&init_ix, ctx.accounts, &[])?;

    // Create meta account
    accs.meta
        .create(&((&*accs).into()), ctx, accs.payer.key, Exempt)?;

    // Initialize spl meta
    accs.spl_metadata.verify_derivation(
        &spl_token_metadata::id(),
        &SplTokenMetaDerivationData {
            mint: *accs.mint.info().key,
        },
    )?;

    // Normalize Token Metadata.
    let name = truncate_utf8(&accs.vaa.name, 32 - 11) + " (Wormhole)";
    let symbol = truncate_utf8(&accs.vaa.symbol, 10);

    let spl_token_metadata_ix =
    ↪   spl_token_metadata::instruction::create_metadata_accounts(
        spl_token_metadata::id(),
        *accs.spl_metadata.key,
        *accs.mint.info().key,
        *accs.mint_authority.info().key,
        *accs.payer.info().key,
        *accs.mint_authority.info().key,
        name,
        symbol,
        String::from(""),
        None,
        0,
        false,
        true,
    );
    invoke_seeded(&spl_token_metadata_ix, ctx, &accs.mint_authority,
↪   None)?;

    // Populate meta account
    accs.meta.chain = accs.vaa.token_chain;
    accs.meta.token_address = accs.vaa.token_address;
    accs.meta.original_decimals = accs.vaa.decimals;

    Ok(())
}

```

- Call Stack

```
fn entrypoint(){// /home/yifei/.cargo/registry/src/github.com-
↪   1ecc6299db9ec823/solana-program-1.7.0/src/entrypoint.rs:46:9: 53:10
↪   }
```

```
    fn instruction::solitaire(){//
    ↪  /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/macros.rs
    ↪  108:14 }
        fn instruction::dispatch(){//
        ↪  /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/macro
        ↪  99:14 }
            fn instruction::CreateWrapped::execute(){//
            ↪  /home/yifei/open/vrust/examples2/wormhole/solana/solitaire/program/src/m
            ↪  74:22 }
                    fn api::create_wrapped::create_wrapped(){//
                    ↪  program/src/api/create_wrapped.rs:108:1: 138:2 }
                        fn api::create_wrapped::create_accounts(){//
                        ↪  program/src/api/create_wrapped.rs:140:1: 198:2
                        ↪  }

```

- description:
- link:
- alleviation:

Appendix

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

Finding Categories

Gas Optimization

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

Mathematical Operations

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

Logical Issue

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

Language Specific

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

Coding Style

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

Checksum Calculation Method

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

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

Disclaimer

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

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you ("Customer" or the "Company") in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without CertiK's prior written consent in each instance.

This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts CertiK to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology. Blockchain technology and cryptographic assets present a high level of ongoing risk. CertiK's position is that each company and individual are responsible for their own due diligence and continuous security. CertiK's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by CertiK is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.