// Security Assessment

04.30.2025 - 05.05.2025

Treasurer Solana program

Nous Research

HALBORN

Treasurer Solana program - Nous Research

Prepared by: HALBORN

Last Updated 07/01/2025

Date of Engagement: April 30th, 2025 - May 5th, 2025

Summary

100% OF ALL REPORTED FINDINGS HAVE BEEN ADDRESSED

ALL FINDINGS	CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
3	0	0	0	0	3

TABLE OF CONTENTS

1. Introduction

`Nous Research team` `Halborn`

psyche

`Treasurer`

`Treasurer`

`Run` `Treasurer`

`Run` `Run`

2. Assessment Summary

`Halborn`

`Nous Research team`

`Implement secure Run authority transfer.`

`Make sure the Run authority signs the Run initialization instruction.`

`Validate the collateral_amount_per_earned_point instruction parameter.`

3. Test Approach And Methodology

4. RISK METHODOLOGY

4.1 EXPLOITABILITY

ATTACK ORIGIN (AO):

ATTACK COST (AC):

ATTACK COMPLEXITY (AX):

METRICS:

EXPLOITABILITY METRIC (M_E)	METRIC VALUE	NUMERICAL VALUE
Attack Origin (AO)	Arbitrary (AO:A) Specific (AO:S)	1 0.2

EXPLOITABILITY METRIC (M_E)	METRIC VALUE	NUMERICAL VALUE
Attack Cost (AC)	Low (AC:L) Medium (AC:M) High (AC:H)	1 0.67 0.33

EXPLOITABILITY METRIC (M_E)	METRIC VALUE	NUMERICAL VALUE
Attack Complexity (AX)	Low (AX:L) Medium (AX:M) High (AX:H)	1 0.67 0.33

E

$$E = \prod m_e$$

4.2 IMPACT

CONFIDENTIALITY (C):

INTEGRITY (I):

AVAILABILITY (A):

DEPOSIT (D):

YIELD (Y):

METRICS:

IMPACT METRIC (M_I)	METRIC VALUE	NUMERICAL VALUE
Confidentiality (C)	None (I:N) Low (I:L) Medium (I:M) High (I:H) Critical (I:C)	0 0.25 0.5 0.75 1
Integrity (I)	None (I:N) Low (I:L) Medium (I:M) High (I:H) Critical (I:C)	0 0.25 0.5 0.75 1
Availability (A)	None (A:N) Low (A:L) Medium (A:M) High (A:H) Critical (A:C)	0 0.25 0.5 0.75 1

IMPACT METRIC (M_I)	METRIC VALUE	NUMERICAL VALUE
Deposit (D)	None (D:N) Low (D:L) Medium (D:M) High (D:H) Critical (D:C)	0 0.25 0.5 0.75 1
Yield (Y)	None (Y:N) Low (Y:L) Medium (Y:M) High (Y:H) Critical (Y:C)	0 0.25 0.5 0.75 1

I

$$I = max(m_I) + \frac{\sum m_I - max(m_I)}{4}$$

4.3 SEVERITY COEFFICIENT

REVERSIBILITY (R):

SCOPE (S):

METRICS:

SEVERITY COEFFICIENT (C)	COEFFICIENT VALUE	NUMERICAL VALUE
Reversibility (r)	None (R:N) Partial (R:P) Full (R:F)	1 0.5 0.25

SEVERITY COEFFICIENT (C)	COEFFICIENT VALUE	NUMERICAL VALUE
Scope (s)	Changed (S:C) Unchanged (S:U)	1.25 1

C

$$C = rs$$

S

$$S = min(10, EIC * 10)$$

SEVERITY	SCORE VALUE RANGE
Critical	9 - 10
High	7 - 8.9
Medium	4.5 - 6.9

SEVERITY	SCORE VALUE RANGE
Low	2 - 4.4
Informational	0 - 1.9

5. SCOPE

FILES AND REPOSITORY

psyche

7a7516b

- ./architectures/decentralized/solana-treasurer/programs/solana-treasurer/src/logic/participant_claim.rs
- ./architectures/decentralized/solana-treasurer/programs/solana-treasurer/src/logic/run_create.rs
- ./architectures/decentralized/solana-treasurer/programs/solana-treasurer/src/state/run.rs

Out-of-Scope:

FILES AND REPOSITORY

psyche

6f684bf

- ./architectures/decentralized/solana-treasurer/Cargo.toml
- ./architectures/decentralized/solana-treasurer/rustfmt.toml
- ./architectures/decentralized/solana-treasurer/Cargo.lock
- ./architectures/decentralized/solana-treasurer/Anchor.toml
- ./architectures/decentralized/solana-treasurer/programs/solana-treasurer/Cargo.toml
- ./architectures/decentralized/solana-treasurer/programs/solana-treasurer/Xargo.toml
- ./architectures/decentralized/solana-treasurer/programs/solana-treasurer/src/lib.rs
- ./architectures/decentralized/solana-treasurer/programs/solana-treasurer/src/logic/mod.rs
- ./architectures/decentralized/solana-treasurer/programs/solana-treasurer/src/logic/run_update.rs
- ./architectures/decentralized/solana-treasurer/programs/solana-treasurer/src/logic/participant_claim.rs
- ./architectures/decentralized/solana-treasurer/programs/solana-treasurer/src/logic/run_create.rs
- ./architectures/decentralized/solana-treasurer/programs/solana-treasurer/src/logic/participant_create.rs
- ./architectures/decentralized/solana-treasurer/programs/solana-treasurer/src/logic/run_top_up.rs
- ./architectures/decentralized/solana-treasurer/programs/solana-treasurer/src/state/run.rs
- ./architectures/decentralized/solana-treasurer/programs/solana-treasurer/src/state/mod.rs
- ./architectures/decentralized/solana-treasurer/programs/solana-treasurer/src/state/participant.rs

Out-of-Scope:

REMEDIATION COMMIT ID:

7a7516b

Out-of-Scope:

6. ASSESSMENT SUMMARY & FINDINGS OVERVIEW

CRITICAL HIGH MEDIUM LOW INFORMATIONAL

SECURITY ANALYSIS	RISK LEVEL	REMEDIATION DATE
THE INSTRUCTION PARAMETER COLLATERAL_AMOUNT_PER_EARNED_POINT IS NOT VALIDATED	INFORMATIONAL	SOLVED - 05/21/2025
THE PROGRAM DOES NOT ALLOW TO TRANSFER THE AUTHORITY OF A RUN	INFORMATIONAL	FUTURE RELEASE
RISK OF LOSING CONTROL OVER THE RUN ACCOUNT	INFORMATIONAL	ACKNOWLEDGED

7. FINDINGS & TECH DETAILS

7.1 THE INSTRUCTION PARAMETER COLLATERAL_AMOUNT_PER_EARNED_POINT IS NOT VALIDATED

// INFORMATIONAL

Description

`run_create` `Run`

`collateral_amount_per_earned_point`

`Run`

```
72  pub fn run_create_processor(
73      context: Context<RunCreateAccounts>,
74      params: RunCreateParams,
75  ) -> Result<()> {
76      let run = &mut context.accounts.run;
77      run.bump = context.bumps.run;
78      run.index = params.index;
79
80      run.main_authority = params.main_authority;
81      run.join_authority = params.join_authority;
82
83      run.coordinator_instance = context.accounts.coordinator_instance.key();
84      run.coordinator_account = context.accounts.coordinator_account.key();
85
86      run.collateral_mint = context.accounts.collateral_mint.key();
87      run.collateral_amount_per_earned_point =
88          params.collateral_amount_per_earned_point;
```

BVSS

Recommendation

`collateral_amount_per_earned_point`

Remediation Comment

`collateral_amount_per_earned_point`

Remediation Hash

7.2 THE PROGRAM DOES NOT ALLOW TO TRANSFER THE AUTHORITY OF A RUN

// INFORMATIONAL

Description

`run_create` `Run`

```rust
pub fn run_create_processor(
    context: Context<RunCreateAccounts>,
    params: RunCreateParams,
) -> Result<()> {
    let run = &mut context.accounts.run;

```

```
        run.bump = context.bumps.run;
        run.index = params.index;

        run.main_authority = params.main_authority;
        run.join_authority = params.join_authority;
```

BVSS

Recommendation

Remediation Comment

7.3 RISK OF LOSING CONTROL OVER THE RUN ACCOUNT

// INFORMATIONAL

Description

`run_create`

```
63  #[derive(AnchorSerialize, AnchorDeserialize, Clone)]
64  pub struct RunCreateParams {
65      pub index: u64,
66      pub run_id: String,
67      pub main_authority: Pubkey,
68      pub join_authority: Pubkey,
69      pub collateral_amount_per_earned_point: u64,
70  }
71
72  pub fn run_create_processor(
73      context: Context<RunCreateAccounts>,
74      params: RunCreateParams,
75  ) -> Result<()> {
76      let run = &mut context.accounts.run;
77      run.bump = context.bumps.run;
78      run.index = params.index;
79
80      run.main_authority = params.main_authority;
81      run.join_authority = params.join_authority;
```

BVSS

Recommendation

Remediation Comment

8. AUTOMATED TESTING

STATIC ANALYSIS REPORT

Description

`cargo audit` `https://crates.io` `cargo audit`

Cargo Audit Results

ID	CRATE	DESCRIPTION
RUSTSEC-2025-0024	crossbeam-channel	crossbeam-channel: double free on Drop
RUSTSEC-2024-0344	curve25519-dalek	Timing variability in `curve25519-dalek` `Scalar29::sub` `Scalar52::sub`
RUSTSEC-2022-0093	ed25519-dalek	Double Public Key Signing Function Oracle Attack on `ed25519-dalek`
RUSTSEC-2025-0022	openssl	Use-After-Free in `Md::fetch` and `Cipher::fetch`
RUSTSEC-2023-0071	rsa	Marvin Attack: potential key recovery through timing sidechannels