Sweat Economy Security Analysis

by Pessimistic

This report is public

September 26, 2022

Abstract

In this report, we consider the security of Sweat Economy project. Our task is to find and describe security issues in the smart contracts of the platform.

Disclaimer

Summary

In this report, we considered the security of Sweat Economy project smart contracts, available in a public GitHub repository. We performed our audit according to the procedure described below.

The audit showed Overpowered role issue of medium severity and two low severity issues.

The project has sufficient documentation. The codebase is thoroughly covered with tests. The overall code quality is good.

After the initial audit, the developers added a pull request with fixes and provided a comment regarding an Overpowered role issue.

Project overview

Project description

For the initial audit, we were provided with Sweat Economy smart contracts on a public GitHub repository, commit 21e6a903b5e30310a63d8a84ced8020c33948342.

The documentation for the project included:

- **README.md** file in the repository.
- Contract overview link on sweat-near wiki.
- **formula_description.pdf** file, sha1sum is `356b3faef6c818dd7e6469a1e087865df08b50e7`.

All 16 tests pass successfully. The code coverage is 94.59%.

Codebase update

After the initial audit, the codebase was updated. For the recheck, we were provided with pull request #41. We reviewed the code at commit 7cdcc0cb5949bc1886b4cb46e151d5744b87a455.

In this update, the developers fixed low-severity issues mentioned in the initial report.

Review procedure

We perform our audit according to the following procedure:

Automated analysis

- We compile the contracts.
- We run tests and calculate the code coverage.
- We scan the project's codebase with cargo-geiger analyzer.
- We manually verify (reject or confirm) all the issues found by the tool.
- We check the project with cargo-audit tool.

Manual analysis

- We manually review the code and assess its quality.
- We check the code for known vulnerabilities.
- We check whether the code logic complies with the provided documentation.
- We suggest possible gas and storage optimizations.

Issues

We are actively looking for:

- Access control issues: incorrect admin or user identification/authorization.
- Lost/stolen assets issues: assets being stuck on the contract or sent to nowhere or to a wrong account.
- DoS due to logical issues: deadlocks, state machine errors, etc.
- DoS due to technical issues: Out-of-Gas error, other limitations.
- Contract interaction issues: reentrancy, insecure calls, caller assumptions, etc.
- Arithmetic issues: overflows, underflows, rounding issues, etc.
- Incorrect Near SDK usage.
- Other issues.

Automated analysis

Automated analysis showed the following:

- **Auto tests**. All 16 tests declared were passed successfully. See the results in Appendix A: Auto tests results.

- **Tests coverage**. For test code coverage calculation, we used cargo-tarpaulin tool. The coverage is 94.59%. For details, see Appendix A: Tests coverage.

- **Check for unsafe Rust code**. We scanned the project with cargo-geiger tool. The tool did not reveal any unsafe code in sweat-near codebase. It showed 16 warnings in near-sdk codebase. However, near-sdk is out of the scope of the audit. For details, see Appendix A: Check for unsafe Rust code.

- **Check for crates vulnerabilities**. We analyzed the project with cargo-audit tool. It showed three vulnerabilities in near-sdk codebase. For details, see Appendix A: Check for crates vulnerabilities.

Manual analysis

We analyzed the modifications of SDK for Sweat token project. There are two main modifications compared to the standard NEP-141 Token implementation:

- NEAR-SDK fork uses shorter map keys for storage, i.e., 32 bytes instead of 64. New type `LookupMapAdapter` is used in all interfaces, which elegantly eliminates a chance to mix new and old interfaces.
- `internal_deposit` function does not result in panic in case of an undefined balance.

Medium severity issues

Medium issues can influence project operation in the current implementation. Bugs, loss of potential income, and other non-critical failures fall into this category, as well as potential problems related to incorrect system management. We highly recommend addressing them.

M01. Overpowered role (commented)

The Contract overview states:

```
Oracle account - an account in an allow-list to provide steps
activity data to the token (call the record_batch contract method).
```

Code logic in **sweat/src/lib.rs** allows the owner to add any oracles that can effectively mint an arbitrary amount of tokens. In the current implementation, the system depends heavily on special accounts. Thus, some scenarios can lead to undesirable consequences for the project and its users, e.g., if the oracle account's private key becomes compromised.

We recommend designing contracts in a trustless manner or implementing proper key management, e.g., setting up a multisig.

> *Comment from the developers: It is our endeavour to deliver trustless movement validators, however, at this stage of technology development it does not appear viable due to unique characteristics of the project. The only way at this stage to deliver trustless architecture would to open source the oracle’s code, which due to nature of its tasks will give advantages to malicious actors and will expose the project to more fraud. Therefore, it is a conscious decision to keep the movement validator’s source code closed and run by Sweatco Ltd. As this part of our technology stack settles and zero knowledge proofs technology matures we believe we will be able to deliver movement validation via trustless oracle(s).*

Low severity issues

Low severity issues do not directly affect project operation. However, they might result in various problems in future code versions. We recommend taking them into account.

L01. Typo in Readme (fixed)

README.md at line 64 includes a `'{"account_id":"ramdom-guy-1.testnet"}'` string as part of command. Consider replacing `ramdom` with `random` since this typo affects demo results.

The issue has been fixed and is not present in the latest version of the code.

L02. Rust version requirements (fixed)

The contract installation requires the Rust version not less than `1.60.0`. However, the installation guide does not mention this requirement.

*The developers specified the requirements for Rust version in **README.md** file.*

Appendix A

A01. Auto tests results

```
running 16 tests
test math::tests::formula_test … ok
test tests::add_oracle_access - should panic … ok
test tests::add_same_oracle - should panic … ok
test tests::add_remove_oracle … ok
test tests::burn … ok
test tests::mint_steps_access_1 - should panic … ok
test tests::minting_steps_access_2 - should panic … ok
test tests::oracle_fee_test … ok
test tests::remove_fake_oracle - should panic … ok
test tests::tge_access_2 - should panic … ok
test tests::tge_access_1 - should panic … ok
test tests::remove_oracle_access - should panic … ok
test tests::tge_liquid … ok
test tests::transfer_to_registered … ok
test tests::transfer_to_unregistered - should panic … ok
test tests::tge_liquid_batch … ok
```

A02. Tests coverage

Uncovered Lines:

- **sweat/src/lib.rs**: 151-152, 161, 166, 173, 175-178, 411, 413, 416, 418.
- **sweat/src/math.rs**: 2.

Tested/Total Lines:

- **sweat/src/lib.rs**: 220/233 +0.00%.
- **sweat/src/math.rs**: 25/26 +0.00%.

94.59% coverage, 245/259 lines covered, +0% change in coverage.

A03. Check for unsafe Rust code

Metric output format: x/y

```
x = unsafe code used by the build
y = total unsafe code found in the crate
```

Symbols:

```
🔒 = No unsafe usage found, declares #![forbid(unsafe_code)]
❓ = No unsafe usage found, missing #![forbid(unsafe_code)]
☢️ = unsafe usage found
```

Functions Expressions Impls Traits Methods Dependency

```
0/0 0/0 0/0 0/0 0/0           ❓ sweat 0.1.0
0/0 0/0 0/0 0/0 0/0           ❓ ├── near-contract-standards 4.0.0
```

```
54/54 479/497 0/0 0/0 0/0        ☢  │   ├── near-sdk 4.0.0
0/0 0/0 0/0 0/0 0/0              🔒 │   │   ├── base64 0.13.0
0/0 7/7 0/0 0/0 0/0              ☢  │   │   ├── borsh 0.9.1
0/0 0/0 0/0 0/0 0/0              ❓ │   │   │   ├── borsh-derive 0.9.1
0/0 0/0 0/0 0/0 0/0              ❓ │   │   │   │   ├── borsh-derive-internal 0.9.1
0/0 0/0 0/0 0/0 0/0              ❓ │   │   │   │   │   ├── proc-macro2 1.0.32
0/0 0/0 0/0 0/0 0/0              🔒 │   │   │   │   │   │   └── unicode-xid 0.2.2
0/0 0/0 0/0 0/0 0/0              ❓ │   │   │   │   │   ├── quote 1.0.10
0/0 0/0 0/0 0/0 0/0              ❓ │   │   │   │   │   │   └── proc-macro2 1.0.32
0/0 45/45 3/3 0/0 2/2            ☢  │   │   │   │   │   └── syn 1.0.78
0/0 0/0 0/0 0/0 0/0              ❓ │   │   │   │   │   ├── proc-macro2 1.0.32
0/0 0/0 0/0 0/0 0/0              ❓ │   │   │   │   │   ├── quote 1.0.10
0/0 0/0 0/0 0/0 0/0              🔒 │   │   │   │   │   └── unicode-xid 0.2.2
0/0 0/0 0/0 0/0 0/0              ❓ │   │   │   │   ├── borsh-schema-derive-internal 0.9.1
0/0 0/0 0/0 0/0 0/0              ❓ │   │   │   │   │   ├── proc-macro2 1.0.32
0/0 0/0 0/0 0/0 0/0              ❓ │   │   │   │   │   ├── quote 1.0.10
0/0 45/45 3/3 0/0 2/2            ☢  │   │   │   │   │   └── syn 1.0.78
0/0 0/0 0/0 0/0 0/0              ❓ │   │   │   │   ├── proc-macro-crate 0.1.5
0/0 0/0 0/0 0/0 0/0              🔒 │   │   │   │   │   └── toml 0.5.8
0/0 5/5 0/0 0/0 0/0              ☢  │   │   │   │   │   └── serde 1.0.136
0/0 0/0 0/0 0/0 0/0              ❓ │   │   │   │   │   └── serde_derive 1.0.136
0/0 0/0 0/0 0/0 0/0              ❓ │   │   │   │   │   ├── proc-macro2 1.0.32
0/0 0/0 0/0 0/0 0/0              ❓ │   │   │   │   │   ├── quote 1.0.10
0/0 45/45 3/3 0/0 2/2            ☢  │   │   │   │   │   └── syn 1.0.78
0/0 0/0 0/0 0/0 0/0              ❓ │   │   │   │   ├── proc-macro2 1.0.32
0/0 45/45 3/3 0/0 2/2            ☢  │   │   │   │   └── syn 1.0.78
2/2 1006/1098 16/19 0/0 35/39    ☢  │   │   │   └── hashbrown 0.9.1
0/0 16/20 0/0 0/0 0/0            ☢  │   │   │   ├── ahash 0.4.7
0/0 5/5 0/0 0/0 0/0              ☢  │   │   │   └── serde 1.0.136
0/0 1/1 0/0 0/0 0/0              ☢  │   │   ├── bs58 0.4.0
12/12 231/231 0/0 0/0 0/0        ☢  │   │   │   └── sha2 0.9.8
0/0 6/6 0/0 0/0 0/0              ☢  │   │   │   ├── block-buffer 0.9.0
0/0 3/3 0/0 0/0 0/0              ☢  │   │   │   │   ├── block-padding 0.2.1
1/1 295/295 20/20 8/8 5/5        ☢  │   │   │   │   └── generic-array 0.14.4
0/0 5/5 0/0 0/0 0/0              ☢  │   │   │   │   ├── serde 1.0.136
0/0 0/0 0/0 0/0 0/0              🔒 │   │   │   │   └── typenum 1.14.0
0/0 0/0 0/0 0/0 0/0              ❓ │   │   │   ├── cfg-if 1.0.0
0/1 0/14 0/0 0/0 0/0             ❓ │   │   │   ├── cpufeatures 0.2.1
0/0 0/0 0/0 0/0 0/0              🔒 │   │   │   ├── digest 0.9.0
1/1 295/295 20/20 8/8 5/5        ☢  │   │   │   │   └── generic-array 0.14.4
0/0 0/0 0/0 0/0 0/0              ❓ │   │   │   └── opaque-debug 0.3.0
0/0 1/1 0/0 0/0 0/0              ☢  │   │   ├── near-crypto 0.13.0
0/0 0/0 0/0 0/0 0/0              ❓ │   │   │   ├── arrayref 0.3.6
0/0 12/21 13/13 1/1 0/0          ☢  │   │   │   ├── blake2 0.9.2
0/0 0/0 0/0 0/0 0/0              🔒 │   │   │   │   ├── crypto-mac 0.8.0
1/1 295/295 20/20 8/8 5/5        ☢  │   │   │   │   │   ├── generic-array 0.14.4
0/0 3/3 0/0 0/0 0/0              ☢  │   │   │   │   │   └── subtle 2.4.1
0/0 0/0 0/0 0/0 0/0              🔒 │   │   │   │   ├── digest 0.9.0
0/0 0/0 0/0 0/0 0/0              ❓ │   │   │   │   └── opaque-debug 0.3.0
0/0 7/7 0/0 0/0 0/0              ☢  │   │   │   ├── borsh 0.9.1
0/0 1/1 0/0 0/0 0/0              ☢  │   │   │   ├── bs58 0.4.0
0/0 0/0 0/0 0/0 0/0              ❓ │   │   │   ├── c2-chacha 0.3.3
0/0 0/0 0/0 0/0 0/0              🔒 │   │   │   │   ├── cipher 0.2.5
1/1 295/295 20/20 8/8 5/5        ☢  │   │   │   │   │   └── generic-array 0.14.4
2/2 636/712 0/0 0/0 17/25        ☢  │   │   │   │   └── ppv-lite86 0.2.16
0/2 0/857 0/0 0/0 0/0            ❓ │   │   │   ├── curve25519-dalek 3.2.0
1/1 193/193 0/0 0/0 0/0          ☢  │   │   │   │   ├── byteorder 1.4.3
```

```
0/0 0/0 0/0 0/0 0/0               🔒 │ │ │ │ ├── digest 0.9.0
0/0 22/22 0/0 0/0 0/0             ☢️ │ │ │ │ ├── rand_core 0.5.1
2/4 50/150 1/1 0/0 3/3            ☢️ │ │ │ │ │ ├── getrandom 0.1.16
0/0 0/0 0/0 0/0 0/0               ❓ │ │ │ │ │ │ ├── cfg-if 1.0.0
0/20 12/353 0/2 0/0 2/38          ☢️ │ │ │ │ │ │ └── libc 0.2.122
0/0 5/5 0/0 0/0 0/0               ☢️ │ │ │ │ │ └── serde 1.0.136
0/0 5/5 0/0 0/0 0/0               ☢️ │ │ │ │ ├── serde 1.0.136
0/0 3/3 0/0 0/0 0/0               ☢️ │ │ │ │ ├── subtle 2.4.1
1/1 22/22 0/0 0/0 0/0             ☢️ │ │ │ │ └── zeroize 1.4.3
0/0 0/0 0/0 0/0 0/0               🔒 │ │ │ │ └── zeroize_derive 1.2.2
0/0 0/0 0/0 0/0 0/0               ❓ │ │ │ │ ├── proc-macro2 1.0.32
0/0 0/0 0/0 0/0 0/0               ❓ │ │ │ │ ├── quote 1.0.10
0/0 45/45 3/3 0/0 2/2             ☢️ │ │ │ │ ├── syn 1.0.78
0/0 0/0 1/1 0/0 0/0               ☢️ │ │ │ │ └── synstructure 0.12.6
0/0 0/0 0/0 0/0 0/0               ❓ │ │ │ │ ├── proc-macro2 1.0.32
0/0 0/0 0/0 0/0 0/0               ❓ │ │ │ │ ├── quote 1.0.10
0/0 45/45 3/3 0/0 2/2             ☢️ │ │ │ │ ├── syn 1.0.78
0/0 0/0 0/0 0/0 0/0               🔒 │ │ │ │ └── unicode-xid 0.2.2
0/0 0/0 0/0 0/0 0/0               ❓ │ │ │ ├── derive_more 0.99.16
0/0 0/0 0/0 0/0 0/0               ❓ │ │ │ │ ├── convert_case 0.4.0
0/0 15/15 0/0 0/0 0/0             ☢️ │ │ │ │ │ └── rand 0.7.3
2/4 50/150 1/1 0/0 3/3            ☢️ │ │ │ │ │ ├── getrandom 0.1.16
0/20 12/353 0/2 0/0 2/38          ☢️ │ │ │ │ │ ├── libc 0.2.122
0/0 0/0 0/0 0/0 0/0               ❓ │ │ │ │ │ ├── rand_chacha 0.2.2
2/2 636/712 0/0 0/0 17/25         ☢️ │ │ │ │ │ │ ├── ppv-lite86 0.2.16
0/0 22/22 0/0 0/0 0/0             ☢️ │ │ │ │ │ │ └── rand_core 0.5.1
0/0 22/22 0/0 0/0 0/0             ☢️ │ │ │ │ │ └── rand_core 0.5.1
0/0 0/0 0/0 0/0 0/0               ❓ │ │ │ │ ├── proc-macro2 1.0.32
0/0 0/0 0/0 0/0 0/0               ❓ │ │ │ │ ├── quote 1.0.10
0/0 45/45 3/3 0/0 2/2             ☢️ │ │ │ │ └── syn 1.0.78
0/0 0/0 0/0 0/0 0/0               🔒 │ │ │ ├── ed25519-dalek 1.0.1
0/2 0/857 0/0 0/0 0/0             ❓ │ │ │ │ ├── curve25519-dalek 3.2.0
0/0 0/0 0/0 0/0 0/0               🔒 │ │ │ │ ├── ed25519 1.3.0
0/0 5/5 0/0 0/0 0/0               ☢️ │ │ │ │ │ ├── serde 1.0.136
0/0 0/0 0/0 0/0 0/0               🔒 │ │ │ │ │ ├── signature 1.5.0
0/0 0/0 0/0 0/0 0/0               🔒 │ │ │ │ │ │ ├── digest 0.10.3
0/0 16/16 0/0 0/0 0/0             ☢️ │ │ │ │ │ │ │ ├── block-buffer 0.10.2
1/1 295/295 20/20 8/8 5/5         ☢️ │ │ │ │ │ │ │ │ └── generic-array 0.14.4
0/0 0/0 0/0 0/0 0/0               🔒 │ │ │ │ │ │ │ ├── crypto-common 0.1.6
1/1 295/295 20/20 8/8 5/5         ☢️ │ │ │ │ │ │ │ │ ├── generic-array 0.14.4
0/0 15/15 0/0 0/0 0/0             ☢️ │ │ │ │ │ │ │ │ ├── rand_core 0.6.3
2/4 50/149 1/1 0/0 3/3            ☢️ │ │ │ │ │ │ │ │ │ ├── getrandom 0.2.3
0/0 0/0 0/0 0/0 0/0               ❓ │ │ │ │ │ │ │ │ │ │ ├── cfg-if 1.0.0
0/20 12/353 0/2 0/0 2/38          ☢️ │ │ │ │ │ │ │ │ │ │ └── libc 0.2.122
0/0 5/5 0/0 0/0 0/0               ☢️ │ │ │ │ │ │ │ │ │ └── serde 1.0.136
0/0 0/0 0/0 0/0 0/0               🔒 │ │ │ │ │ │ │ │ └── typenum 1.14.0
0/0 3/3 0/0 0/0 0/0               ☢️ │ │ │ │ │ │ │ └── subtle 2.4.1
0/0 15/15 0/0 0/0 0/0             ☢️ │ │ │ │ │ │ └── rand_core 0.6.3
1/1 22/22 0/0 0/0 0/0             ☢️ │ │ │ │ │ └── zeroize 1.4.3
0/0 15/15 0/0 0/0 0/0             ☢️ │ │ │ │ ├── rand 0.7.3
0/0 22/22 0/0 0/0 0/0             ☢️ │ │ │ │ ├── rand_core 0.5.1
0/0 5/5 0/0 0/0 0/0               ☢️ │ │ │ │ ├── serde 1.0.136
12/12 231/231 0/0 0/0 0/0         ☢️ │ │ │ │ ├── sha2 0.9.8
1/1 22/22 0/0 0/0 0/0             ☢️ │ │ │ │ └── zeroize 1.4.3
0/20 12/353 0/2 0/0 2/38          ☢️ │ │ │ ├── libc 0.2.122
0/0 0/0 0/0 0/0 0/0               ❓ │ │ │ ├── near-account-id 0.13.0
0/0 7/7 0/0 0/0 0/0               ☢️ │ │ │ │ ├── borsh 0.9.1
```

```
0/0 5/5 0/0 0/0 0/0             ☢️ │   │   │   │   └── serde 1.0.136
1/1 74/93 4/6 0/0 2/3           ☢️ │   │   │   ├── once_cell 1.10.0
0/0 215/215 2/2 0/0 0/0         ☢️ │   │   │   ├── parity-secp256k1 0.7.0
4/4 295/295 2/2 1/1 5/5         ☢️ │   │   │   │   ├── arrayvec 0.5.2
0/0 5/5 0/0 0/0 0/0             ☢️ │   │   │   │   │   └── serde 1.0.136
0/0 15/15 0/0 0/0 0/0           ☢️ │   │   │   │   └── rand 0.7.3
0/0 0/0 0/0 0/0 0/0             ❓ │   │   │   ├── primitive-types 0.10.1
0/0 0/0 0/0 0/0 0/0             ❓ │   │   │   │   ├── fixed-hash 0.7.0
1/1 193/193 0/0 0/0 0/0         ☢️ │   │   │   │   │   ├── byteorder 1.4.3
0/0 14/30 0/0 0/0 0/0           ☢️ │   │   │   │   │   ├── rand 0.8.4
0/20 12/353 0/2 0/0 2/38        ☢️ │   │   │   │   │   │   ├── libc 0.2.122
0/0 0/0 0/0 0/0 0/0             ❓ │   │   │   │   │   │   ├── rand_chacha 0.3.1
2/2 636/712 0/0 0/0 17/25       ☢️ │   │   │   │   │   │   │   ├── ppv-lite86 0.2.16
0/0 15/15 0/0 0/0 0/0           ☢️ │   │   │   │   │   │   │   ├── rand_core 0.6.3
0/0 5/5 0/0 0/0 0/0             ☢️ │   │   │   │   │   │   │   └── serde 1.0.136
0/0 15/15 0/0 0/0 0/0           ☢️ │   │   │   │   │   │   ├── rand_core 0.6.3
0/0 5/5 0/0 0/0 0/0             ☢️ │   │   │   │   │   │   └── serde 1.0.136
0/0 0/0 0/0 0/0 0/0             ❓ │   │   │   │   │   ├── rustc-hex 2.1.0
0/0 0/0 0/0 0/0 0/0             ❓ │   │   │   │   │   └── static_assertions 1.1.0
0/0 0/0 0/0 0/0 0/0             ❓ │   │   │   │   ├── impl-codec 0.5.1
0/0 4/4 0/0 0/0 0/0             ☢️ │   │   │   │   │   └── parity-scale-codec 2.3.1
2/2 350/350 2/2 0/0 7/7         ☢️ │   │   │   │   │   ├── arrayvec 0.7.2
0/0 5/5 0/0 0/0 0/0             ☢️ │   │   │   │   │   │   └── serde 1.0.136
15/15 1105/1108 14/14 1/1 62/62 ☢️ │   │   │   │   │   ├── bitvec 0.20.4
0/0 0/0 0/0 0/0 0/0             ❓ │   │   │   │   │   │   ├── funty 1.1.0
0/0 0/0 0/0 0/0 0/0             ❓ │   │   │   │   │   │   ├── radium 0.6.2
0/0 5/5 0/0 0/0 0/0             ☢️ │   │   │   │   │   │   ├── serde 1.0.136
0/0 0/0 0/0 0/0 0/0             ❓ │   │   │   │   │   │   ├── tap 1.0.1
0/0 0/0 0/0 0/0 0/0             ❓ │   │   │   │   │   │   └── wyz 0.2.0
0/0 0/0 2/2 3/3 0/0             ☢️ │   │   │   │   │   ├── byte-slice-cast 1.2.0
1/1 295/295 20/20 8/8 5/5       ☢️ │   │   │   │   │   ├── generic-array 0.14.4
0/0 0/0 0/0 0/0 0/0             ❓ │   │   │   │   │   ├── impl-trait-for-tuples 0.2.1
0/0 0/0 0/0 0/0 0/0             ❓ │   │   │   │   │   │   ├── proc-macro2 1.0.32
0/0 0/0 0/0 0/0 0/0             ❓ │   │   │   │   │   │   ├── quote 1.0.10
0/0 45/45 3/3 0/0 2/2           ☢️ │   │   │   │   │   │   └── syn 1.0.78
0/0 0/0 0/0 0/0 0/0             ❓ │   │   │   │   │   ├── parity-scale-codec-derive 2.3.1
0/0 0/0 0/0 0/0 0/0             ❓ │   │   │   │   │   │   ├── proc-macro-crate 1.1.0
0/0 0/0 0/0 0/0 0/0             ❓ │   │   │   │   │   │   │   ├── thiserror 1.0.30
0/0 0/0 0/0 0/0 0/0             ❓ │   │   │   │   │   │   │   │   └── thiserror-impl 1.0.30
0/0 0/0 0/0 0/0 0/0             ❓ │   │   │   │   │   │   │   │   ├── proc-macro2 1.0.32
0/0 0/0 0/0 0/0 0/0             ❓ │   │   │   │   │   │   │   │   ├── quote 1.0.10
0/0 45/45 3/3 0/0 2/2           ☢️ │   │   │   │   │   │   │   │   └── syn 1.0.78
0/0 0/0 0/0 0/0 0/0             🔒 │   │   │   │   │   │   │   └── toml 0.5.8
0/0 0/0 0/0 0/0 0/0             ❓ │   │   │   │   │   │   ├── proc-macro2 1.0.32
0/0 0/0 0/0 0/0 0/0             ❓ │   │   │   │   │   │   ├── quote 1.0.10
0/0 45/45 3/3 0/0 2/2           ☢️ │   │   │   │   │   │   └── syn 1.0.78
0/0 5/5 0/0 0/0 0/0             ☢️ │   │   │   │   │   └── serde 1.0.136
0/0 0/0 0/0 0/0 0/0             ❓ │   │   │   │   └── uint 0.9.1
1/1 193/193 0/0 0/0 0/0         ☢️ │   │   │   │   ├── byteorder 1.4.3
0/0 0/0 0/0 0/0 0/0             ❓ │   │   │   │   ├── crunchy 0.2.2
0/0 0/0 0/0 0/0 0/0             ❓ │   │   │   │   ├── hex 0.4.3
0/0 5/5 0/0 0/0 0/0             ☢️ │   │   │   │   │   └── serde 1.0.136
0/0 15/15 0/0 0/0 0/0           ☢️ │   │   │   │   ├── rand 0.7.3
0/0 0/0 0/0 0/0 0/0             ❓ │   │   │   │   └── static_assertions 1.1.0
0/0 15/15 0/0 0/0 0/0           ☢️ │   │   │   ├── rand 0.7.3
0/0 22/22 0/0 0/0 0/0           ☢️ │   │   │   ├── rand_core 0.5.1
0/0 5/5 0/0 0/0 0/0             ☢️ │   │   │   ├── serde 1.0.136
```

```
0/0 4/7 0/0 0/0 0/0                ☢️ │   │   │   ├── serde_json 1.0.71
0/0 1/1 0/0 0/0 0/0                ☢️ │   │   │   │   ├── itoa 0.4.8
8/12 674/921 0/0 0/0 2/2           ☢️ │   │   │   │   ├── ryu 1.0.5
0/0 5/5 0/0 0/0 0/0                ☢️ │   │   │   │   └── serde 1.0.136
0/0 3/3 0/0 0/0 0/0                ☢️ │   │   │   ├── subtle 2.4.1
0/0 0/0 0/0 0/0 0/0                ❓ │   │   │   └── thiserror 1.0.30
0/0 0/0 0/0 0/0 0/0                ❓ │   │   ├── near-primitives 0.13.0
0/0 7/7 0/0 0/0 0/0                ☢️ │   │   │   ├── borsh 0.9.1
1/1 193/193 0/0 0/0 0/0            ☢️ │   │   │   ├── byteorder 1.4.3
0/0 0/0 0/0 0/0 0/0                ❓ │   │   │   ├── bytesize 1.1.0
0/0 5/5 0/0 0/0 0/0                ☢️ │   │   │   │   └── serde 1.0.136
1/1 44/90 2/2 0/0 0/0              ☢️ │   │   │   ├── chrono 0.4.19
0/20 12/353 0/2 0/0 2/38           ☢️ │   │   │   │   ├── libc 0.2.122
0/0 0/0 0/0 0/0 0/0                ❓ │   │   │   │   ├── num-integer 0.1.44
0/0 4/10 0/0 0/0 0/0               ☢️ │   │   │   │   │   └── num-traits 0.2.14
0/0 4/10 0/0 0/0 0/0               ☢️ │   │   │   │   ├── num-traits 0.2.14
0/0 5/5 0/0 0/0 0/0                ☢️ │   │   │   │   ├── serde 1.0.136
1/1 216/216 0/0 0/0 0/0            ☢️ │   │   │   │   └── time 0.1.43
0/20 12/353 0/2 0/0 2/38           ☢️ │   │   │   │   └── libc 0.2.122
0/0 0/0 0/0 0/0 0/0                ❓ │   │   │   ├── derive_more 0.99.16
0/0 0/0 0/0 0/0 0/0                🔒 │   │   │   ├── easy-ext 0.2.9
0/0 0/0 0/0 0/0 0/0                ❓ │   │   │   ├── hex 0.4.3
0/0 1/1 0/0 0/0 0/0                ☢️ │   │   │   ├── near-crypto 0.13.0
0/0 0/0 0/0 0/0 0/0                ❓ │   │   │   ├── near-primitives-core 0.13.0
0/0 0/0 0/0 0/0 0/0                🔒 │   │   │   │   ├── base64 0.11.0
0/0 7/7 0/0 0/0 0/0                ☢️ │   │   │   │   ├── borsh 0.9.1
0/0 1/1 0/0 0/0 0/0                ☢️ │   │   │   │   ├── bs58 0.4.0
0/0 0/0 0/0 0/0 0/0                ❓ │   │   │   │   ├── derive_more 0.99.16
0/0 0/0 0/0 0/0 0/0                ❓ │   │   │   │   ├── near-account-id 0.13.0
0/0 0/0 0/0 0/0 0/0                ❓ │   │   │   │   ├── num-rational 0.3.2
0/0 6/11 0/0 0/0 0/0               ☢️ │   │   │   │   │   ├── num-bigint 0.3.3
0/0 0/0 0/0 0/0 0/0                ❓ │   │   │   │   │   │   ├── num-integer 0.1.44
0/0 4/10 0/0 0/0 0/0               ☢️ │   │   │   │   │   │   ├── num-traits 0.2.14
0/0 15/15 0/0 0/0 0/0              ☢️ │   │   │   │   │   │   ├── rand 0.7.3
0/0 5/5 0/0 0/0 0/0                ☢️ │   │   │   │   │   │   └── serde 1.0.136
0/0 0/0 0/0 0/0 0/0                ❓ │   │   │   │   │   ├── num-integer 0.1.44
0/0 4/10 0/0 0/0 0/0               ☢️ │   │   │   │   │   ├── num-traits 0.2.14
0/0 5/5 0/0 0/0 0/0                ☢️ │   │   │   │   │   └── serde 1.0.136
0/0 5/5 0/0 0/0 0/0                ☢️ │   │   │   │   ├── serde 1.0.136
8/8 196/196 0/0 0/0 0/0            ☢️ │   │   │   │   ├── sha2 0.10.2
0/0 0/0 0/0 0/0 0/0                ❓ │   │   │   │   │   ├── cfg-if 1.0.0
0/1 0/14 0/0 0/0 0/0               ❓ │   │   │   │   │   ├── cpufeatures 0.2.1
0/0 0/0 0/0 0/0 0/0                🔒 │   │   │   │   │   └── digest 0.10.3
0/0 0/0 0/0 0/0 0/0                ❓ │   │   │   │   └── strum 0.24.1
0/0 0/0 0/0 0/0 0/0                ❓ │   │   │   │   └── strum_macros 0.24.3
0/0 0/0 0/0 0/0 0/0                🔒 │   │   │   │   ├── heck 0.4.0
0/0 0/0 0/0 0/0 0/0                ❓ │   │   │   │   ├── proc-macro2 1.0.32
0/0 0/0 0/0 0/0 0/0                ❓ │   │   │   │   ├── quote 1.0.10
0/1 0/1 0/0 0/0 0/0                ❓ │   │   │   │   ├── rustversion 1.0.9
0/0 45/45 3/3 0/0 2/2              ☢️ │   │   │   │   └── syn 1.0.78
0/0 0/0 0/0 0/0 0/0                ❓ │   │   │   ├── near-rpc-error-macro 0.13.0
0/0 0/0 0/0 0/0 0/0                ❓ │   │   │   │   ├── near-rpc-error-core 0.13.0
0/0 0/0 0/0 0/0 0/0                ❓ │   │   │   │   │   ├── quote 1.0.10
0/0 5/5 0/0 0/0 0/0                ☢️ │   │   │   │   │   ├── serde 1.0.136
0/0 45/45 3/3 0/0 2/2              ☢️ │   │   │   │   │   └── syn 1.0.78
0/0 5/5 0/0 0/0 0/0                ☢️ │   │   │   │   ├── serde 1.0.136
0/0 4/7 0/0 0/0 0/0                ☢️ │   │   │   │   ├── serde_json 1.0.71
```

```
0/0 45/45 3/3 0/0 2/2              ☢ │ │ │ │ └── syn 1.0.78
0/0 0/0 0/0 0/0 0/0                ❓ │ │ │ ├── near-vm-errors 0.13.0
0/0 7/7 0/0 0/0 0/0                ☢ │ │ │ │ ├── borsh 0.9.1
0/0 0/0 0/0 0/0 0/0                ❓ │ │ │ │ ├── near-account-id 0.13.0
0/0 0/0 0/0 0/0 0/0                ❓ │ │ │ │ ├── near-rpc-error-macro 0.13.0
0/0 5/5 0/0 0/0 0/0                ☢ │ │ │ │ └── serde 1.0.136
0/0 0/0 0/0 0/0 0/0                ❓ │ │ │ ├── num-rational 0.3.2
1/1 74/93 4/6 0/0 2/3              ☢ │ │ │ ├── once_cell 1.10.0
0/0 0/0 0/0 0/0 0/0                ❓ │ │ │ ├── primitive-types 0.10.1
0/0 15/15 0/0 0/0 0/0              ☢ │ │ │ ├── rand 0.7.3
0/0 151/151 0/0 0/0 0/0            ☢ │ │ │ ├── reed-solomon-erasure 4.0.2
0/20 12/353 0/2 0/0 2/38           ☢ │ │ │ │ ├── libc 0.2.122
1/1 392/392 7/7 1/1 13/13          ☢ │ │ │ │ └── smallvec 1.7.0
0/0 5/5 0/0 0/0 0/0                ☢ │ │ │ │ └── serde 1.0.136
0/0 5/5 0/0 0/0 0/0                ☢ │ │ │ ├── serde 1.0.136
0/0 4/7 0/0 0/0 0/0                ☢ │ │ │ ├── serde_json 1.0.71
0/0 0/0 0/0 0/0 0/0                ❓ │ │ │ ├── smart-default 0.6.0
0/0 0/0 0/0 0/0 0/0                ❓ │ │ │ │ ├── proc-macro2 1.0.32
0/0 0/0 0/0 0/0 0/0                ❓ │ │ │ │ ├── quote 1.0.10
0/0 45/45 3/3 0/0 2/2              ☢ │ │ │ │ └── syn 1.0.78
0/0 0/0 0/0 0/0 0/0                ❓ │ │ │ ├── strum 0.24.1
0/0 0/0 0/0 0/0 0/0                ❓ │ │ │ └── thiserror 1.0.30
0/0 0/0 0/0 0/0 0/0                ❓ │ │ ├── near-primitives-core 0.13.0
0/0 0/0 0/0 0/0 0/0                ❓ │ │ ├── near-sdk-macros 4.0.0
0/0 0/0 0/0 0/0 0/0                ❓ │ │ │ ├── Inflector 0.11.4
0/0 0/0 0/0 0/0 0/0                ❓ │ │ │ ├── proc-macro2 1.0.32
0/0 0/0 0/0 0/0 0/0                ❓ │ │ │ ├── quote 1.0.10
0/0 45/45 3/3 0/0 2/2              ☢ │ │ │ └── syn 1.0.78
1/1 1/1 0/0 0/0 0/0                ☢ │ │ ├── near-sys 0.2.0
0/0 9/9 0/0 0/0 0/0                ☢ │ │ ├── near-vm-logic 0.13.0
0/0 0/0 0/0 0/0 0/0                🔒 │ │ │ ├── base64 0.13.0
0/0 7/7 0/0 0/0 0/0                ☢ │ │ │ ├── borsh 0.9.1
0/0 1/1 0/0 0/0 0/0                ☢ │ │ │ ├── bs58 0.4.0
1/1 193/193 0/0 0/0 0/0            ☢ │ │ │ ├── byteorder 1.4.3
0/0 0/0 0/0 0/0 0/0                ❓ │ │ │ ├── near-account-id 0.13.0
0/0 1/1 0/0 0/0 0/0                ☢ │ │ │ ├── near-crypto 0.13.0
0/0 0/0 0/0 0/0 0/0                ❓ │ │ │ ├── near-primitives 0.13.0
0/0 0/0 0/0 0/0 0/0                ❓ │ │ │ ├── near-primitives-core 0.13.0
0/0 0/0 0/0 0/0 0/0                ❓ │ │ │ ├── near-vm-errors 0.13.0
0/0 0/0 0/0 0/0 0/0                🔒 │ │ │ ├── ripemd 0.1.1
0/0 0/0 0/0 0/0 0/0                🔒 │ │ │ │ └── digest 0.10.3
0/0 5/5 0/0 0/0 0/0                ☢ │ │ │ ├── serde 1.0.136
8/8 196/196 0/0 0/0 0/0            ☢ │ │ │ ├── sha2 0.10.2
0/0 14/14 0/0 0/0 0/0              ☢ │ │ │ └── sha3 0.9.1
0/0 6/6 0/0 0/0 0/0                ☢ │ │ │ ├── block-buffer 0.9.0
0/0 0/0 0/0 0/0 0/0                🔒 │ │ │ ├── digest 0.9.0
0/0 0/0 0/0 0/0 0/0                ❓ │ │ │ ├── keccak 0.1.0
0/0 0/0 0/0 0/0 0/0                ❓ │ │ │ └── opaque-debug 0.3.0
1/1 74/93 4/6 0/0 2/3              ☢ │ │ ├── once_cell 1.10.0
0/0 5/5 0/0 0/0 0/0                ☢ │ │ ├── serde 1.0.136
0/0 4/7 0/0 0/0 0/0                ☢ │ │ ├── serde_json 1.0.71
3/5 460/570 4/4 1/1 21/25          ☢ │ │ └── wee_alloc 0.4.5
0/0 0/0 0/0 0/0 0/0                ❓ │ │ ├── cfg-if 0.1.10
0/20 12/353 0/2 0/0 2/38           ☢ │ │ ├── libc 0.2.122
0/0 0/0 0/0 0/0 0/0                ❓ │ │ └── memory_units 0.4.0
0/0 5/5 0/0 0/0 0/0                ☢ │ ├── serde 1.0.136
0/0 4/7 0/0 0/0 0/0                ☢ │ └── serde_json 1.0.71
```

```
54/54 479/497 0/0 0/0 0/0         ☢  ├── near-sdk 4.0.0
0/0 0/0 0/0 0/0 0/0               ❓ └── static_assertions 1.1.0

122/156 7370/9436 94/101 16/16 179/232
```

error: Found 16 warnings.

A04. Check for crates vulnerabilities

```
Fetching advisory database from `https://github.com/RustSec/advisory-db.git`
Loaded 452 security advisories (from /home/gsg/.cargo/advisory-db)
Updating crates.io index
Scanning Cargo.lock for vulnerabilities (325 crate dependencies)
```

```
Crate: chrono
Version: 0.4.19
Title: Potential segfault in localtime_r invocations
Date: 2020-11-10
ID: RUSTSEC-2020-0159
URL: https://rustsec.org/advisories/RUSTSEC-2020-0159
Solution: Upgrade to >=0.4.20

Dependency tree:
chrono 0.4.19
├── workspaces 0.2.0
│ └── examples 0.0.0
├── near-sandbox-utils 0.2.0
│ └── workspaces 0.2.0
├── near-primitives 0.13.0
│ ├── near-vm-logic 0.13.0
│ │ └── near-sdk 4.0.0
│ │ ├── sweat 0.1.0
│ │ ├── near-contract-standards 4.0.0
│ │ │ └── sweat 0.1.0
│ │ └── examples 0.0.0
│ └── near-sdk 4.0.0
├── near-primitives 0.12.0
│ ├── workspaces 0.2.0
│ ├── near-network-primitives 0.12.0
│ │ ├── near-jsonrpc-primitives 0.12.0
│ │ │ ├── workspaces 0.2.0
│ │ │ ├── near-jsonrpc-client 0.3.0
│ │ │ └── workspaces 0.2.0
│ │ ├── near-client-primitives 0.12.0
│ │ └── near-jsonrpc-primitives 0.12.0
│ ├── near-jsonrpc-primitives 0.12.0
│ ├── near-jsonrpc-client 0.3.0
│ ├── near-client-primitives 0.12.0
│ ├── near-chain-primitives 0.12.0
│ │ ├── near-client-primitives 0.12.0
│ │ ├── near-chunks-primitives 0.12.0
│ │ └── near-client-primitives 0.12.0
│ └── near-chain-configs 0.12.0
│ ├── near-jsonrpc-primitives 0.12.0
│ ├── near-jsonrpc-client 0.3.0
│ └── near-client-primitives 0.12.0
├── near-network-primitives 0.12.0
├── near-client-primitives 0.12.0
├── near-chain-primitives 0.12.0
└── near-chain-configs 0.12.0
```

```
Crate: regex
Version: 1.5.4
Title: Regexes with large repetitions on empty sub-expressions take a very
long time to parse
Date: 2022-03-08
ID: RUSTSEC-2022-0013
URL: https://rustsec.org/advisories/RUSTSEC-2022-0013
Solution: Upgrade to >=1.5.5
```

```
Dependency tree:
regex 1.5.4
├── prometheus 0.11.0
│ └── near-metrics 0.12.0
│ └── near-jsonrpc-primitives 0.12.0
│ ├── workspaces 0.2.0
│ │ └── examples 0.0.0
│ └── near-jsonrpc-client 0.3.0
│ └── workspaces 0.2.0
└── near-units-core 0.2.0
├── near-units-macro 0.2.0
│ └── near-units 0.2.0
│ └── examples 0.0.0
└── near-units 0.2.0
```

```
Crate: time
Version: 0.1.43
Title: Potential segfault in the time crate
Date: 2020-11-18
ID: RUSTSEC-2020-0071
URL: https://rustsec.org/advisories/RUSTSEC-2020-0071
Solution: Upgrade to >=0.2.23
```

```
Dependency tree:
time 0.1.43
├── zip 0.5.13
│ └── binary-install 0.0.2
│ └── near-sandbox-utils 0.2.0
│ └── workspaces 0.2.0
│ └── examples 0.0.0
└── chrono 0.4.19
├── workspaces 0.2.0
├── near-sandbox-utils 0.2.0
├── near-primitives 0.13.0
│ ├── near-vm-logic 0.13.0
│ │ └── near-sdk 4.0.0
│ │ ├── sweat 0.1.0
│ │ ├── near-contract-standards 4.0.0
│ │ │ └── sweat 0.1.0
│ │ └── examples 0.0.0
│ └── near-sdk 4.0.0
├── near-primitives 0.12.0
│ ├── workspaces 0.2.0
│ ├── near-network-primitives 0.12.0
│ │ ├── near-jsonrpc-primitives 0.12.0
│ │ │ ├── workspaces 0.2.0
│ │ │ ├── near-jsonrpc-client 0.3.0
│ │ │ └── workspaces 0.2.0
│ │ └── near-client-primitives 0.12.0
│ │ └── near-jsonrpc-primitives 0.12.0
│ ├── near-jsonrpc-primitives 0.12.0
│ ├── near-jsonrpc-client 0.3.0
│ ├── near-client-primitives 0.12.0
│ ├── near-chain-primitives 0.12.0
│   │   ├── near-client-primitives 0.12.0
│   │   └── near-chunks-primitives 0.12.0
│   │   └── near-client-primitives 0.12.0
│   └── near-chain-configs 0.12.0
│   ├── near-jsonrpc-primitives 0.12.0
│   ├── near-jsonrpc-client 0.3.0
│   └── near-client-primitives 0.12.0
├── near-network-primitives 0.12.0
├── near-client-primitives 0.12.0
├── near-chain-primitives 0.12.0
└── near-chain-configs 0.12.0

Crate: failure
Version: 0.1.8
Warning: unmaintained
Title: failure is officially deprecated/unmaintained
Date: 2020-05-02
ID: RUSTSEC-2020-0036
URL: https://rustsec.org/advisories/RUSTSEC-2020-0036

Dependency tree:
failure 0.1.8
├── near-chain-primitives 0.12.0
│   ├── near-client-primitives 0.12.0
│   │   └── near-jsonrpc-primitives 0.12.0
│   │   ├── workspaces 0.2.0
│   │   │   └── examples 0.0.0
│   │   └── near-jsonrpc-client 0.3.0
│   │   └── workspaces 0.2.0
│   └── near-chunks-primitives 0.12.0
│   └── near-client-primitives 0.12.0
└── binary-install 0.0.2
└── near-sandbox-utils 0.2.0
└── workspaces 0.2.0
```

error: 3 vulnerabilities found!

warning: 1 allowed warning found.

This analysis was performed by Pessimistic:

Sergey Grigoriev, Security Engineer
Evgeny Marchenko, Senior Security Engineer
Boris Nikashin, Analyst
Alexander Seleznev, Founder

September 26, 2022