CERTIK

Security Assessment

Walken.io

Apr 27th, 2022

Table of Contents

Summary

Overview

- Project Summary
- Audit Summary
- Vulnerability Summary
- Audit Scope

Understandings

- System overview
- External Dependencies
- Privileged Functions

Findings

- CKP-01 : Unused `mint_address` Field
- PRO-01 : Lack of Owner Check for Token Account
- PRO-02 : Lack of Input Validation on `spl_token_program`
- PRO-03 : Lack of Input Validation on `Sysvar` and `System Program`
- PRO-04 : Missing Emit Events

Appendix

Disclaimer

About

Summary

This report has been prepared for Walken.io to discover issues and vulnerabilities in the source code of the Walken.io 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	Walken.io
Platform	Solana
Language	Rust
Codebase	https://github.com/walken-io/token-vesting
Commit	• e222214b069f41c0e1e2c75694659409e4475cb4

Audit Summary

Delivery Date	Apr 27, 2022 UTC
Audit Methodology	Static Analysis, Manual Review

Vulnerability Summary

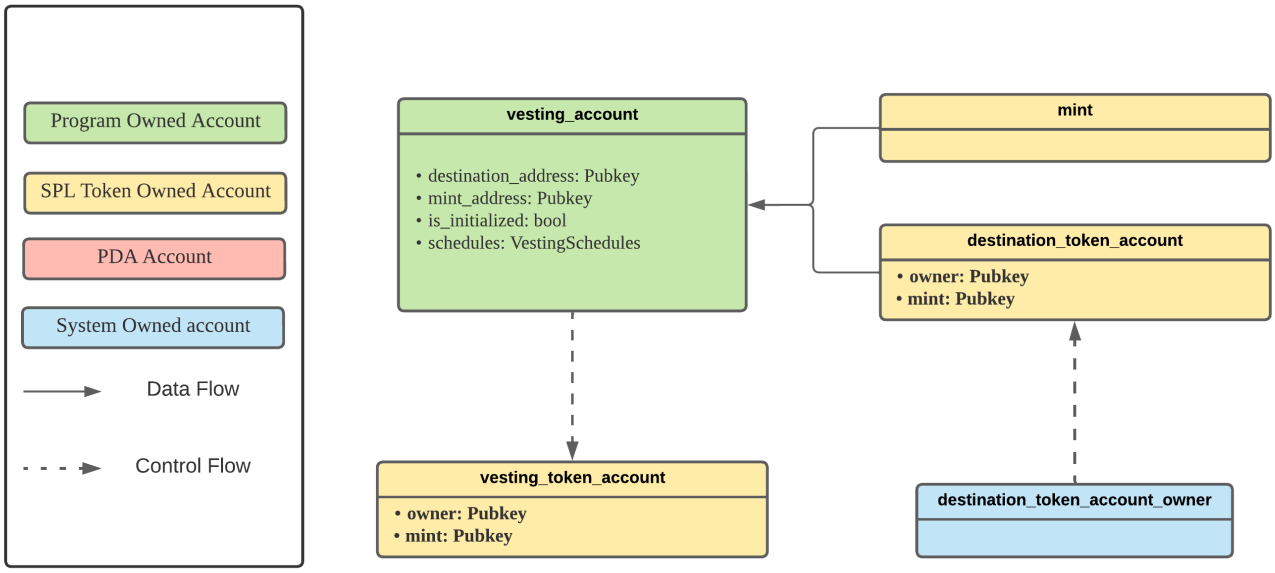
Vulnerability Level	Total	Pending	Declined	Acknowledged	Mitigated	Partially Resolved	Resolved
Critical	0	0	0	0	0	0	0
Major	0	0	0	0	0	0	0
Medium	0	0	0	0	0	0	0
Minor	2	0	0	2	0	0	0
Informational	3	0	0	3	0	0	0
Discussion	0	0	0	0	0	0	0

Audit Scope

ID	File	SHA256 Checksum
LIB	program/src/lib.rs	ddd41d939725dfb0dd8fe7c42993a3ad1bcd95d06d0af5fd3cb97384740cbf55
ERR	program/src/error.rs	6cda011e0517db456bf86beb44cd12d063078e558660c75351755e090ae885b5
PRO	program/src/processor.rs	80bddd0e8de0c71126db9705be9c44eda66445e01ac98adfac95daa152e9baaa
INS	program/src/instruction.rs	9e83b6a29563a347fce0bb6f6f78773f07bffad9e580c209f194ff86054c3bbe
ENT	program/src/entrypoint.rs	37e8b9b305c5dde93beaba3e9613ff508a55d1117fa2865bebd55a927e32bbf4
STA	program/src/state.rs	b4d66f35f007fb2de9206898cdf6c4ca0b59a3f64a22264794347f5c80fc6786

Understandings

System overview



External Dependencies

The project mainly contains the following dependencies:

Dependency	Version
solana-program	1.6.22
spl-token	3.0.1
solana-frozen-abi	=1.6.24
spl-associated-token-account	1.0.2
arrayref	0.3.6
num=derive	0.3
num-traits	0.2
thiserror	1.0.24
arbitrary	0.4
honggfuzz	0.5

Dependency	Version
solana=sdk	=1.6.24

We assume these dependencies are valid and non-vulnerable factors and implement proper logic to collaborate with the current project.

It should be noted here that the code dependencies are actively developed in the current auditing version. It is necessary to keep the dependencies up-to-date to avoid potential vulnerabilities. For example, the `spl-token` v3.0.1 will not check the program id which may cause unexpected problems.

The on-chain program can be upgradeable after the initial deployment based on Solana's features. Also, based on the unique rent mechanism in Solana, the balance in the account should be carefully set.

Privileged Functions

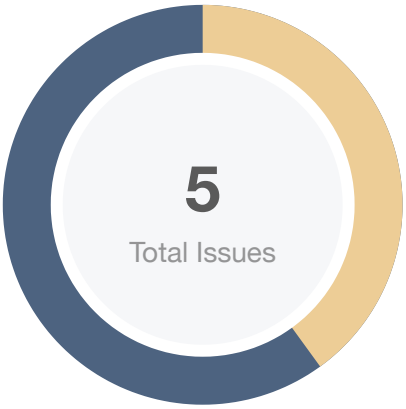
The program `token-vesting` contains the following privileged functions/instructions:

- `source_token_account_owner` can init `token_vesting` account data via `process_create`.
- `destination_token_account_owner` can change `token_vesting`'s `destination_token_account` via `process_change_destination`.

Additionally, if the program is upgradeable, the upgrade authority account can upgrade the contract/program, thus causing unexpected consequences.

To improve the trustworthiness of the project, dynamic runtime updates in the project should be notified to the community.

Findings



Critical	0 (0.00%)
Major	0 (0.00%)
Medium	0 (0.00%)
Minor	2 (40.00%)
Informational	3 (60.00%)
Discussion	0 (0.00%)

ID	Title	Category	Severity	Status
CKP-01	Unused `mint_address` Field	Coding Style	Informational	Acknowledged
PRO-01	Lack Of Owner Check For Token Account	Logical Issue	Informational	Acknowledged
PRO-02	Lack Of Input Validation On `spl_token_program`	Logical Issue	Minor	Acknowledged
PRO-03	Lack Of Input Validation On `Sysvar` And `System Program`	Language Specific	Minor	Acknowledged
PRO-04	Missing Emit Events	Coding Style	Informational	Acknowledged

CKP-01 | Unused `mint_address` Field

Category	Severity	Location	Status
Coding Style	Informational	program/src/state.rs: 17; program/src/processor.rs: 72, 320	Acknowledged

Description

The `mint_address` is not used in the current codebase, which should be used to validate the mint field for the `vesting_token_account`, `destination_token_address` and `source_token_account` in the instruction `process_create`, and the `new_destination_token_account` in the instruction `process_change_destination`. This could help the program prevent transaction failures from the incorrect setup.

Recommendation

Recommend adding the aforementioned mint validations for better security practice.

Alleviation

[Walken.io]: The team acknowledged this issue and decided not to change the current codebase at this stage.

PRO-01 | Lack Of Owner Check For Token Account

Category	Severity	Location	Status
Logical Issue	Informational	program/src/processor.rs: 84, 86, 280	Acknowledged

Description

In the functions `process_create` and `process_change_destination`, an owner check is lacking for the following accounts.

- `vesting_token_account`
- `source_token_account`
- `new_destination_token_account`

Recommendation

Recommend adding the owner check for the aforementioned accounts, for example,

```
if source_token_account.owner != &spl_token::id(){
  return Err(...)
}
```

Alleviation

[Walken.io]: The team acknowledged this issue and decided not to change the current codebase at this stage.

PRO-02 | Lack Of Input Validation On `spl_token_program`

Category	Severity	Location	Status
Logical Issue	Minor	program/src/processor.rs: 82	Acknowledged

Description

In the function `process_create`, it will transfer tokens to the `vesting_token_account` and `spl_token_account.key` will be used as `spl_token` program id.

```
164         let transfer_tokens_to_vesting_account = transfer(
165             spl_token_account.key,
166             source_token_account.key,
167             vesting_token_account.key,
168             source_token_account_owner.key,
169             &[],
170             total_amount,
171         )?;
```

It is necessary to check if the provided `spl_token` is the authenticated token program on-chain (e.g., checking against `spl_token::id()` or `TokenkegQfeZyiNwAJbNbGKPFXCWuBvf9Ss623VQ5DA`. Furthermore, the current project uses SPL-Token v3.0.1, which does not have a built-in check for the SPL-Token program id.

Recommendation

Recommend adding aforementioned validation on `spl_token_account.key` and keep dependency(spl-token) up to date.

Alleviation

[Walken.io]: The team acknowledged this issue and decided not to change the current codebase at this stage.

PRO-03 | Lack Of Input Validation On `Sysvar` And `System Program`

Category	Severity	Location	Status
Language Specific	Minor	program/src/processor.rs: 36, 37, 193	Acknowledged

Description

The `token vesting` program is interact with following `Sysvar`/`System Program` but lack of validation may cause unexpected results:

- `system_program_account` should equal to `11111111111111111111111111111111`
- `rent_sysvar_account` should equal to `SysvarRent111111111111111111111111111111`
- `clock_sysvar_account` should equal to `SysvarC1ock11111111111111111111111111111`

Reference: Sysvar Cluster Data

Recommendation

Recommend adding aforementioned validations for `Sysvar` and `System Program` accounts.

Alleviation

[Walken.io]: The team acknowledged this issue and decided not to change the current codebase at this stage.

PRO-04 | Missing Emit Events

Category	Severity	Location	Status
Coding Style	Informational	program/src/processor.rs: 28, 72, 185, 270	Acknowledged

Description

The following four functions that affect the status of sensitive variables (e.g., the `vesting_account`) should be able to emit events.

- `process_init()`
- `process_create()`
- `process_unlock()`
- `process_change_destination()`

Recommendation

Recommend adding events for sensitive actions and emitting them in the functions.

Alleviation

[Walken.io]: The team acknowledged this issue and decided not to change the current codebase at this stage.

Appendix

Finding Categories

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

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.

ALL SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF ARE PROVIDED "AS IS" AND "AS

AVAILABLE" AND WITH ALL FAULTS AND DEFECTS WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, CERTIK HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS. WITHOUT LIMITING THE FOREGOING, CERTIK SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND ALL WARRANTIES ARISING FROM COURSE OF DEALING, USAGE, OR TRADE PRACTICE. WITHOUT LIMITING THE FOREGOING, CERTIK MAKES NO WARRANTY OF ANY KIND THAT THE SERVICES, THE LABELS, THE ASSESSMENT REPORT, WORK PRODUCT, OR OTHER MATERIALS, OR ANY PRODUCTS OR RESULTS OF THE USE THEREOF, WILL MEET CUSTOMER'S OR ANY OTHER PERSON'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULT, BE COMPATIBLE OR WORK WITH ANY SOFTWARE, SYSTEM, OR OTHER SERVICES, OR BE SECURE, ACCURATE, COMPLETE, FREE OF HARMFUL CODE, OR ERROR-FREE. WITHOUT LIMITATION TO THE FOREGOING, CERTIK PROVIDES NO WARRANTY OR UNDERTAKING, AND MAKES NO REPRESENTATION OF ANY KIND THAT THE SERVICE WILL MEET CUSTOMER'S REQUIREMENTS, ACHIEVE ANY INTENDED RESULTS, BE COMPATIBLE OR WORK WITH ANY OTHER SOFTWARE, APPLICATIONS, SYSTEMS OR SERVICES, OPERATE WITHOUT INTERRUPTION, MEET ANY PERFORMANCE OR RELIABILITY STANDARDS OR BE ERROR FREE OR THAT ANY ERRORS OR DEFECTS CAN OR WILL BE CORRECTED.

WITHOUT LIMITING THE FOREGOING, NEITHER CERTIK NOR ANY OF CERTIK'S AGENTS MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED AS TO THE ACCURACY, RELIABILITY, OR CURRENCY OF ANY INFORMATION OR CONTENT PROVIDED THROUGH THE SERVICE. CERTIK WILL ASSUME NO LIABILITY OR RESPONSIBILITY FOR (I) ANY ERRORS, MISTAKES, OR INACCURACIES OF CONTENT AND MATERIALS OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY CONTENT, OR (II) ANY PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM CUSTOMER'S ACCESS TO OR USE OF THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS.

ALL THIRD-PARTY MATERIALS ARE PROVIDED "AS IS" AND ANY REPRESENTATION OR WARRANTY OF OR CONCERNING ANY THIRD-PARTY MATERIALS IS STRICTLY BETWEEN CUSTOMER AND THE THIRD-PARTY OWNER OR DISTRIBUTOR OF THE THIRD-PARTY MATERIALS.

THE SERVICES, ASSESSMENT REPORT, AND ANY OTHER MATERIALS HEREUNDER ARE SOLELY PROVIDED TO CUSTOMER AND MAY NOT BE RELIED ON BY ANY OTHER PERSON OR FOR ANY PURPOSE NOT SPECIFICALLY IDENTIFIED IN THIS AGREEMENT, NOR MAY COPIES BE DELIVERED TO, ANY OTHER PERSON WITHOUT CERTIK'S PRIOR WRITTEN CONSENT IN EACH INSTANCE.

NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING

MATERIALS AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH SERVICES, ASSESSMENT REPORT, AND ANY ACCOMPANYING MATERIALS.

THE REPRESENTATIONS AND WARRANTIES OF CERTIK CONTAINED IN THIS AGREEMENT ARE SOLELY FOR THE BENEFIT OF CUSTOMER. ACCORDINGLY, NO THIRD PARTY OR ANYONE ACTING ON BEHALF OF ANY THEREOF, SHALL BE A THIRD PARTY OR OTHER BENEFICIARY OF SUCH REPRESENTATIONS AND WARRANTIES AND NO SUCH THIRD PARTY SHALL HAVE ANY RIGHTS OF CONTRIBUTION AGAINST CERTIK WITH RESPECT TO SUCH REPRESENTATIONS OR WARRANTIES OR ANY MATTER SUBJECT TO OR RESULTING IN INDEMNIFICATION UNDER THIS AGREEMENT OR OTHERWISE.

FOR AVOIDANCE OF DOUBT, THE SERVICES, INCLUDING ANY ASSOCIATED ASSESSMENT REPORTS OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

About

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we're able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.

