SECURICHAIN

SMART CONTRACT AUDIT

SECURITY ANALYSIS REPORT
FOR

TERRAVERSE NETWORK

April 12th , 2022

SECURICHAIN

Security Rating

The rating is based on the number, severity and latest status of detected issues

Terraverse Network

SECURICHAIN

Disclaimer

This report containing confidential information which can be used internally by the Customer, or it can be disclosed publicly after all vulnerabilities are fixed — upon a decision of the Customer.

SecuriChain does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed.

The report in no way provides investment advice, nor should be leveraged as investment advice of any sort.

Terraverse Network

SECURICHAIN

TABLE OF CONTENTS

Terraverse Network

SECURICHAIN

VULNERABILITY ASSESSMENT OVERVIEW

1.1. ASSIGNING RISK LEVELS

The Auditor categorizes each of the detected vulnerabilities into 4 levels (High, Medium, Low, and Info) according to the degree of the risks it may cause in the Customer's operations. For details of the rating standards, please refer to "Appendix 2 Risk Rating." Please also note that the assessment of the findings is based on Auditor's own perspective and may contain speculations in some cases.

SECURICHAIN

1.2. SCOPE OF WORK

Project Name	**Terraverse**
Platform	**Terra**
Languages	**Rust**
Methods	**Automation scan, architecture review, functional testing, manual code review**
Repository	**terraverse-linear-staking** Github: https://github.com/terraverse-network/terraverse-linear-staking Commit: 178d469 **terraverse-pool-ido** Github: https://github.com/terraverse-network/terraverse-pool-ido Commit: bbad4c9 **terraverse-pool-maker** Github: https://github.com/terraverse-network/terraverse-pool-maker Commit: d85f8a0
Documents	
Timelines	March 21st - April 12th

Terraverse Network

SECURICHAIN

1.3. CHECKSUM FILE

TERRAVERSE-LINEAR-STAKING

No.	Hash	Name
1	bc52feae7243d023b107c299c3c4d7322c9d6547ffedf33105e260af7c1e836b	Cargo.lock
2	991e7607e27faab53ddfc3920ae54aff7afc287ec87dd471bf0c32002f5da618	Cargo.toml
3	6a72b31a10cb3c5a5004cdf68e88b1b02215715ab77791eb6f3f1ddbc0964bf2	rustfmt.toml
4	514a7da45cd95ec4bee4ab91c691c6e728fcde1b590d891263913ed671f76357	api.rs
5	d658e3454589bfadcb03353ee7fb6f7290fd933d4626c4578bc6ac60dd81c619	contract.rs
6	2239fadcb10ef4e6cbe715b23265bf3502aa931fe7c375641584b6630baa889c	error.rs
7	812622c1448bc9a6a37cf502b1228237c7d84675e5837a619d99ca1337fd101c	integration_tests.rs
8	690696018c534274c0a90d57da25f06a011884a1a04b8ce4114fa257e1e28f99	lib.rs
9	af5e4b3508f3657bd280c756d72c3fdae6a282ae6d02c9239cb43145f584c177	msg.rs
10	cbcb11a4ee21c2291bca18e92a30633b53e03df738db8507e698bed4cc7a207f	state.rs

SECURICHAIN

1.3. CHECKSUM FILE

TERRAVERSE-POOL-IDO

No.	Hash	Name
1	df8993ba89585a1f6248738be372aedfc76b51be1e052d54ece61666ce0a1244	Cargo.lock
2	ef841b4387e0d5ceafdb842dbff2441731e1dff0f4ab0a86f97454e358fb6a39	Cargo.toml
3	6a72b31a10cb3c5a5004cdf68e88b1b02215715ab77791eb6f3f1ddbc0964bf2	rustfmt.toml
4	c3bd181bacb4e62b775f739a61475633bed6ced1f630d77fed4f43fd6df0448b	contract.rs
5	0dd0b7b4eba1a656dac4c0a3a55cc910d729e95cd9189188faeb2c1d695154f5	error.rs
6	3e62212e93a5008c18b7fc78e39daf6821c044ee6b54ae2f8d0f30ac15f20fd8	lib.rs
7	086b6a677779f26c1f33b59b9bf9d315fa3fcb45f1e4a1723366640598fc93a5	msg.rs
8	e601165565ee008dd19b17f042e07194d1dcbb26415f95277db94ab659799b38	state.rs

SECURICHAIN

1.3. CHECKSUM FILE

TERRAVERSE-POOL-MAKER

No.	Hash	Name
1	238663215d9545bcb9eae67cf6f062efd621140cfea5a093fd0c39bd56955e42	Cargo.lock
2	ed9229aa92f9f9ce1fbe345eadb671863fd6411548642d531579bf39ff3d980a	Cargo.toml
3	6a72b31a10cb3c5a5004cdf68e88b1b02215715ab77791eb6f3f1ddbc0964bf2	rustfmt.toml
4	f20933f938be1e919d582e107393f009d8e41fa4663759c714878f1ea22f2e18	signature.py
5	8234311f845fb8f4c5ec58a5c9369d332f647de8a1e507e9557423b0401dce1e	contract.rs
6	b2614598217f625bd74d5b86f3e6f9c65ef2c0a5e470f2cf32a4c65f4c90b829	error.rs
7	3e62212e93a5008c18b7fc78e39daf6821c044ee6b54ae2f8d0f30ac15f20fd8	lib.rs
8	36e08b78c6fc84a428970afd98b0bd64a07958953c9fa407f1829090c589fd21	msg.rs
9	f838442ec8f2872ac06642e4d65697a26d8352bf919da7d199c2c6955d64ddce	state.rs

SECURICHAIN

1.4. ASSESSMENT RESULTS

According to the assessment, the Customer's smart contracts have a security rating of 97/100

RATE	DESCRIPTION
96-100	**No vulnerabilities** were found or all detected ones have been resolved
70-95	Unresolved **Low-level** vulnerabilities exist
40-69	Unresolved **Medium-level** vulnerabilities exist
0-39	Unresolved **High-level** vulnerabilities exist

For more information on criteria for risk rating, refer to Appendix.2

SECURICHAIN

FINDINGS

2.1 List of Vulnerabilities

The detected vulnerabilities are listed below. Please refer to "Appendix.2 Risk Rating" for the risk assessment method.

Vulnerabilities distributed in the smart contract

ID	Risk Level	Name	Amount	Status
SC1	**Information**	Outdated Dependencies	3	Resolved
SC2	**Low**	Duplicate Function Call	1	Resolved
SC3	**Medium**	Allows to claim all purchased tokens in one go	1	Resolved

For rating of each vulnerability, refer to Appendix 2.

SECURICHAIN

2.1 Details

[1] Outdated Dependencies

Information: 3

Overview

The libraries and dependencies used in smart contracts are outdated and potential security risks.

Description

An attacker can take advantage of insecure code contained in outdated libraries and dependencies to attack smart contracts.

Library / Dependence	Current	Latest
serde	1.0.127	1.0.136
generic-array	0.14.4	0.14.5
syn	1.0.74	1.0.90
rand_core	0.5.1	0.6.3
getrandom	0.1.16	0.2.6
libc	0.2.99	0.2.121
zeroize	1.4.1	1.5.4
serde_json	1.0.66	1.0.79
sha2	0.9.5	0.10.2
dyn-clone	1.0.4	1.0.5
serde-json-wasm	0.3.1	0.4.0
itoa	0.4.7	1.0.1
block-buffer	0.9.0	0.10.2

2.1 Details

Recommendation

Update the latest libraries and dependencies.

Location

- terraverse-linear-staking: Cargo.lock, Cargo.toml
- terraverse-pool-ido: Cargo.lock, Cargo.toml
- terraverse-pool-maker: Cargo.lock, Cargo.toml

SECURICHAIN

2.1 Details

[2] Duplicate Function Call

Low: 1

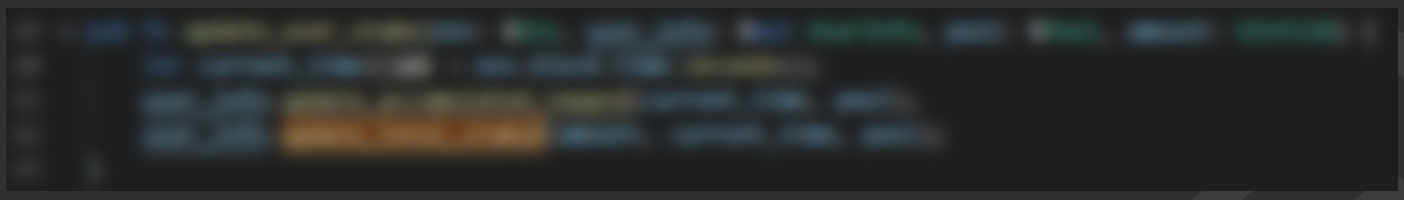
Overview

Function `state.rs::update_accumulated_reward()` duplicated call-in function `api.rs::update_user_stake()`.
Returned data as well as calculated data may not return as expected, gas cost will increase (if any).

Impossible Impacts

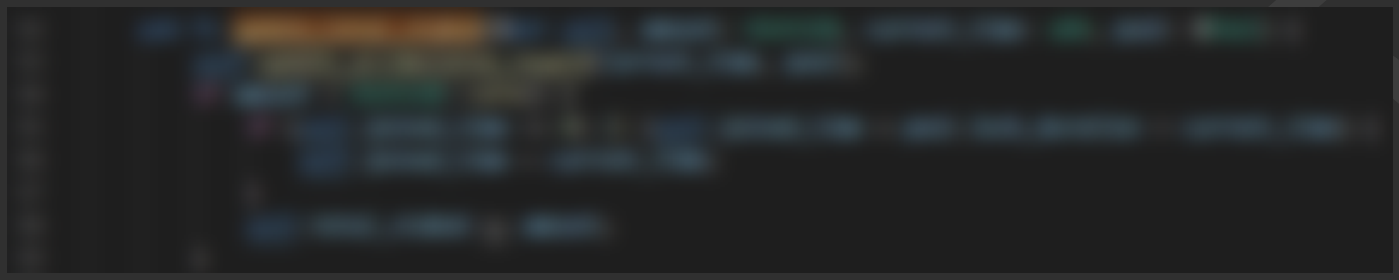
The `update_user_stake` function in the api.rs file is calling two functions, `update_accumulated_reward` and `update_total_staked in state.rs file. However, `update_accumulated_reward` function is also called in `update_total_staked` thus resulting in duplicate.

[terraverse-linear-staking::api.rs#L22]



Blurred image of the code snippet in the public report due to the Customer's code being in the private repository)

[terraverse-linear-staking::api.rs#L53]



Blurred image of the code snippet in the public report due to the Customer's code being in the private repository)

SECURICHAIN

2.1 Details

Recommendation

Remove line 53 in file terraverse-linear staking::api.rs

Location

terraverse-linear-staking::api.rs#L53

SECURICHAIN

[3] Business Vulnerability: (Allows to claim all purchased tokens in one go.)

Medium: 1

Overview

According to General Logic, the token claim must be divided into several times.

Posible Impacts

Function `user_claim` allows users to claim `amount` tokens and can claim all purchased tokens in one go.

Blurred image of the code snippet in the public report due to the Customer's code being in the private repository)

Recommendation

Check the `amount` of tokens claim.

Location

terraverse-pool-ido::contract.rs#L145-L172

SECURICHAIN

CONCLUSION

This document, and its appendices, represent our best effort to capture the results of several days of intensive activity.

Smart contracts within the scope were analyzed with static analysis tools and manually reviewed.

Please feel free to direct any questions on this assessment to: audit@securichain.io

SECURICHAIN

APPENDIX 1: ASSESSMENT LIST

	CHECKLIST	
Arithmetic operations	Integer Overflow/Underflow	Integer Overflow/Underflow
	Integer Truncation	Integer Sign
	Wrong Operator	
Re-entrancy		
Bad Randomness	Timestamp Dependence	Blockhash
Front running		
DDos	DOS By Complex Fallback Function	DOS By Gaslimit
	DOS By Non-existent Address Or Malicious Contract	
Gas usage	Invariants in Loop	Invariants State Variables Are Not Declared Constant
Unsafe external calls		
Business Logics Review		
Access Control & Authorization	Replay Attack	Use tx.origin For Authentication
Logic Vulnerability		

SECURICHAIN

APPENDIX 2: LIST RATING

Risk Level	Explain	Example Types
High	The issue puts a large number of users' sensitive information at risk, or is reasonably likely to lead to catastrophic impact for client's reputation or serious financial implications for client and users.	Re-entrancy Front running DDos Bad Randomness Logic Vulnerability Arithmetic operations
Medium	The issue puts a subset of users' sensitive information at risk, would be detrimental for the client's reputation if exploited, or is reasonably likely to lead to moderate financial impact.	Access Control Unsafe external calls Business Logics Review Logic Vulnerability
Low	The risk is relatively small and could not be exploited on a recurring basis, or is a risk that the client has indicated is low impact in view of the client's business circumstances.	Gas Usage
Info	The issue does not pose an immediate risk, but is relevant to security best practices or Defense in Depth.	Blockhash