VIBRANIUM AUDITS

Security Assessment

TechTrees

Vibranium Audits Verified on Oct 22nd, 2022

Vibranium Audits Verified on Oct 22nd, 2022

Techtrees

The security assessment was prepared by Vibranium Audits, the leader in Web 3.0 security.

Executive Summary

TYPES	ECOSYSTEM	METHODS
DeFi	BSC	Manual Review, Static Analysis

LANGUAGE	TIMELINE	KEY COMPONENTS
Solidity	Delivered on 10/22/2022	N/A

CODEBASE

Private Repository

https://bscscan.com/address/0x6a684b3578f5b07c0aa02fafc33ed248ae0c2db2

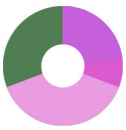
...View All

COMMITS

aab075ed32a93586e1dea5da17acff47dbb12aec68c723ad1172f4770aaef06860ae540f02945a01

...View All

Vulnerability Summary



13	2	1	1	9	0	0
Total Findings	Resolved	Mitigated	Partially Resolved	Acknowledged	Declined	Unresolved

0	Critical		Critical risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks.
3	Major	1 Mitigated, 2 Acknowledged	Major risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project.
1	Medium	1 Partially Resolved	Medium risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform.
5	Minor	1 Resolved, 4 Acknowledged	Minor risks can be any of the above, but on a smaller scale. They generally do not compromise the overall integrity of the project, but they may be less efficient than other solutions.
4	Informational	1 Resolved, 3 Acknowledged	Informational errors are often recommendations to improve the style of the code or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

TABLE OF CONTENTS | TECHTREES

Summary

Executive Summary

Vulnerability Summary

Codebase

Audit Scope

Approach & Methods

Findings

TTC-01 : Initial Token Distribution

TTC-02 : Centralization Risks in TechTreesCoin.sol

TTC-03 : Centralization Risks in TechTreesCoinStaking.sol

TTC-04 : Inconsistent Logic

TTC-05 : Missing Zero Address Validation

TTC-06 : Usage of `transfer`/`send` for sending Ether

TTC-07 : Unchecked ERC-20 `transfer()`/`transferFrom()` Call

TTC-08 : `initTokens()` Can Be Called Multiple Times

TTT-01 : Lack of reasonable boundary

TCK-01 : Missing Emit Events (Arithmetic Parameter)

TCK-02 : Lack of Documentation

TTT-02 : Too Many Digits

TTT-03 : Whitelist privileges kept when transferring ownership

Optimizations

TTC-09 : Unnecessary Use of SafeMath

TTC-10 : Unused State Variable

Formal Verification

Considered Functions And Scope

Verification Results

Appendix

Disclaimer

CODEBASE | TECHTREES

Repository

Private Repository

https://bscscan.com/address/0x6a684b3578f5b07c0aa02fafc33ed248ae0c2db2

https://github.com/TechTreeCoin/staking

Commit

aab075ed32a93586e1dea5da17acff47dbb12aec

68c723ad1172f4770aaef06860ae540f02945a01

AUDIT SCOPE | TECHTREES

3 files audited ● 2 files with Acknowledged findings ● 1 file without findings

ID	File	SHA256 Checksum
TTC	staking/TechTreesCoinStaking.sol	82f0412b9f98247d46db328443b6472e2e967fa5a02e6698185e82b4338a874c
TTT	TechTreesCoin.sol	c406798c770020609c0a6ca74554c3a3c9e17e6433a57c051714d0959c96b11c
IPT	interfaces/IPoint.sol	5093451f38e6833203264e636d4f92ca1f97abd5f7e53def3111a61a6513c533

APPROACH & METHODS | TECHTREES

This report has been prepared for Techtrees to discover issues and vulnerabilities in the source code of the Techtrees project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Manual Review and Static Analysis techniques.

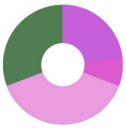
The auditing process pays special attention to the following considerations:

- 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:

- Testing the smart contracts against both common and uncommon attack vectors;
- 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.

FINDINGS | TECHTREES



13	0	3	1	5	4
Total Findings	Critical	Major	Medium	Minor	Informational

This report has been prepared to discover issues and vulnerabilities for Techtrees. Through this audit, we have uncovered 13 issues ranging from different severity levels. Utilizing the techniques of Manual Review & Static Analysis to complement rigorous manual code reviews, we discovered the following findings:

ID	Title	Category	Severity	Status
TTC-01	**Initial Token Distribution**	**Centralization / Privilege**	**Major**	**Mitigated**
TTC-02	**Centralization Risks In TechTreesCoin.Sol**	**Centralization / Privilege**	**Major**	**Acknowledged**
TTC-03	**Centralization Risks In TechTreesCoinStaking.Sol**	**Centralization / Privilege**	**Major**	**Acknowledged**
TTC-04	Inconsistent Logic	Logical Issue, Volatile Code	Medium	Partially Resolved
TTC-05	Missing Zero Address Validation	Volatile Code	Minor	Acknowledged
TTC-06	Usage Of `transfer` / `send` For Sending Ether	Volatile Code	Minor	Acknowledged
TTC-07	Unchecked ERC-20 `transfer()` / `transferFrom()` Call	Volatile Code	Minor	Acknowledged
TTC-08	`initTokens()` Can Be Called Multiple Times	Volatile Code, Logical Issue	Minor	Resolved
TTT-01	Lack Of Reasonable Boundary	Volatile Code	Minor	Acknowledged
TCK-01	Missing Emit Events (Arithmetic Parameter)	Language Specific	Informational	Resolved
TCK-02	Lack Of Documentation	Coding Style	Informational	Acknowledged

ID	Title	Category	Severity	Status
TTT-02	Too Many Digits	Coding Style	Informational	Acknowledged
TTT-03	Whitelist Privileges Kept When Transferring Ownership	Logical Issue	Informational	Acknowledged

TTC-01 | INITIAL TOKEN DISTRIBUTION

Category	Severity	Location	Status
Centralization / Privilege	**Major**	**0×6a684b3578f5b07c0aa02fafc33ed248ae0c2db2 (address): 1252**	**Mitigated**

Description

Tokens are sent to the deployer when deploying the contract. This could be a centralization risk as the deployer can distribute tokens without obtaining the consensus of the community.

Recommendation

We recommend the team to be transparent regarding the initial token distribution process, and the team shall make enough efforts to restrict the access of the private key.

Alleviation

[Vibranium Audits]: The initial token distribution has been documented in commit68c723ad1172f4770aaef06860ae540f02945a01.

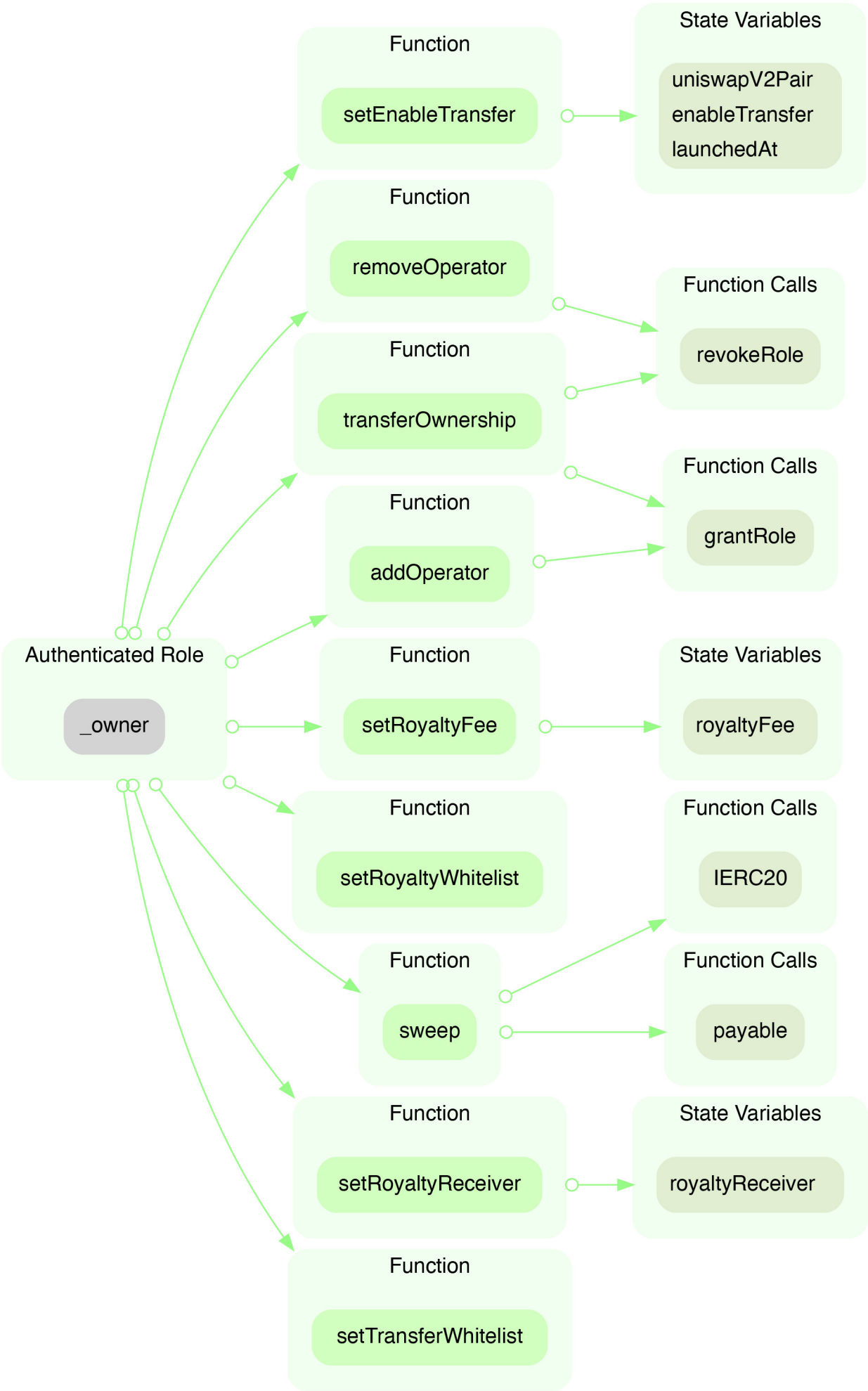
TTC-02 | CENTRALIZATION RISKS IN TECHTREESCOIN.SOL

Category	Severity	Location	Status
Centralization / Privilege	**Major**	**0×6a684b3578f5b07c0aa02fafc33ed248ae0c2db2 (address): 647, 655, 937, 1323, 1327, 1331, 1337, 1344, 1351, 1355, 1359, 1370**	**Acknowledged**

Description

In the contract `TechTreesCoin` the role `_owner` has authority over the functions shown in the diagram below. Any compromise to the `_owner` account may allow the hacker to take advantage of this authority, allowing them to receive all future tokens by:

1. removing all users in the royalty whitelist;
2. setting themselves as the royalty receiver;
3. setting the royalty fee to 100%.


Function
setEnableTransfer
State Variables
uniswapV2Pair
enableTransfer
launchedAt
Function
removeOperator
Function Calls
revokeRole
Function
transferOwnership
Function Calls
grantRole
Function
addOperator
Authenticated Role
_owner
Function
setRoyaltyFee
State Variables
royaltyFee
Function
setRoyaltyWhitelist
Function Calls
IERC20
Function
sweep
Function Calls
payable
Function
setRoyaltyReceiver
State Variables
royaltyReceiver
Function
setTransferWhitelist

The risk describes the current project design and potentially makes iterations to improve in the security operation and level of decentralization, which in most cases cannot be resolved entirely at the present stage. We advise the client to carefully manage the privileged account's private key to avoid any potential risks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., multisignature wallets. Indicatively, here are some feasible suggestions that would also mitigate the potential risk at a different level in terms of short-term, long-term and permanent:

Short Term:

Timelock and Multi sign (⅔, ⅗) combination *mitigate* by delaying the sensitive operation and avoiding a single point of key management failure.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
  AND
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key compromised;
  AND
- A medium/blog link for sharing the timelock contract and multi-signers addresses information with the public audience.

Long Term:

Timelock and DAO, the combination, *mitigate* by applying decentralization and transparency.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
  AND
- Introduction of a DAO/governance/voting module to increase transparency and user involvement.
  AND
- A medium/blog link for sharing the timelock contract, multi-signers addresses, and DAO information with the public audience.

Permanent:

Renouncing the ownership or removing the function can be considered *fully resolved*.

- Renounce the ownership and never claim back the privileged roles.
  OR
- Remove the risky functionality.

Alleviation

`[TechTrees]`: Issue acknowledged. I will fix the issue in the future, which will not be included in this audit engagement. We plan to renounce the ownership, and it is mentioned in the whitepaper available publicly.

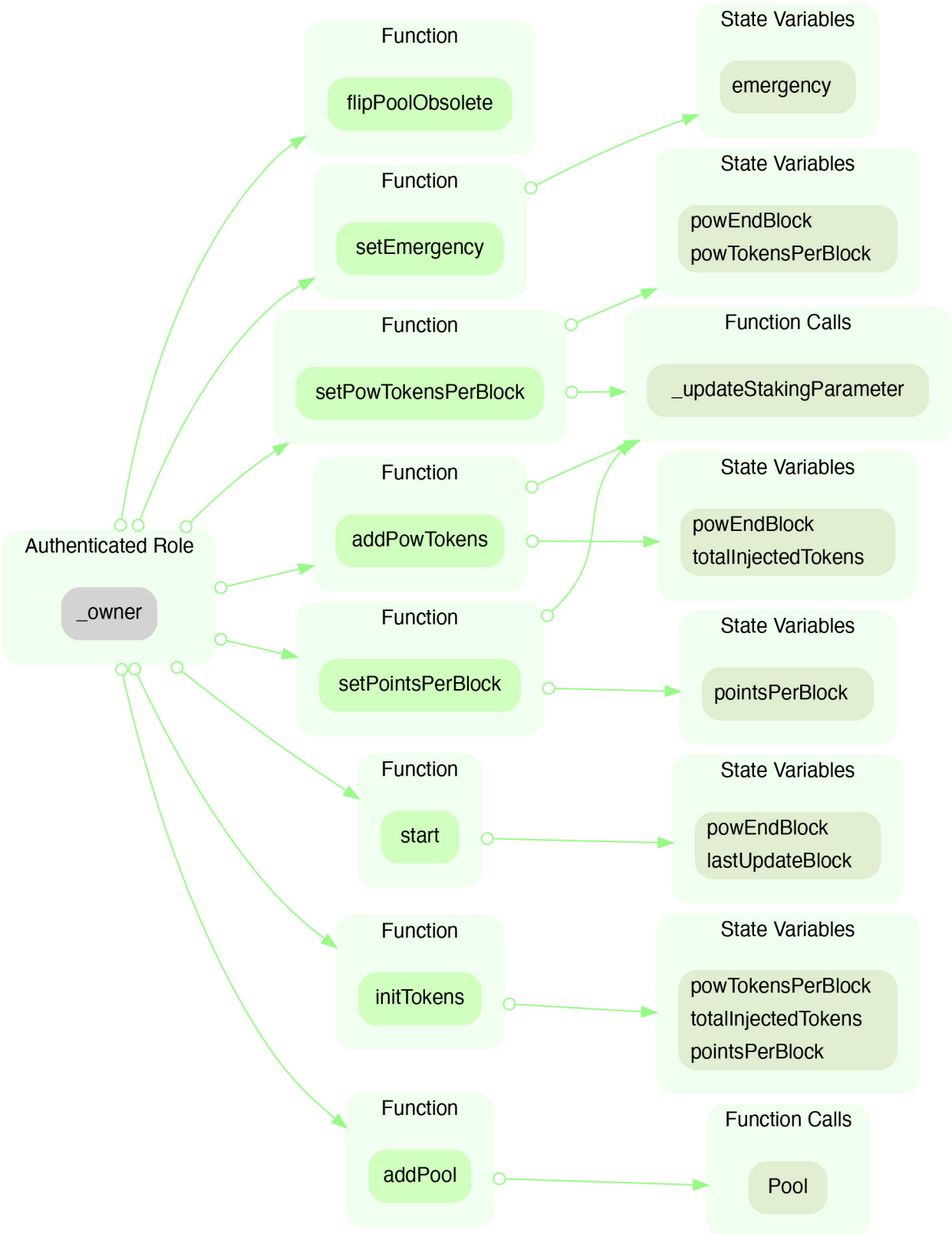
TTC-03 | CENTRALIZATION RISKS IN TECHTREESCOINSTAKING.SOL

Category	Severity	Location	Status
Centralization / Privilege	**Major**	**TechTreesCoinStaking.sol#L73-L73--:-73;-TechTreesCoinStaking.sol#L85-L85--:85;-TechTreesCoinStaking.sol#L97-L97):-97;-TechTreesCoinStaking.sol#L104-L104--CertiKP-roject):-104;-TechTreesCoinStaking.sol#L113-L113--C-ertiKProject):-113;-TechTreesCoinStaking.sol#L120-L120--):-120;-TechTreesCoinStaking.sol#L134-L134--):-134;-TechTreesCoinStakin-g.sol#L138-L138--):-138**	**Acknowledged**

Description

In the contract `TechTreesCoinStaking` the role `_owner` has authority over the functions shown in the diagram below. Any compromise to the `_owner` account may allow the hacker to take advantage of this authority and:

- mark every existing pool as obsolete;
- set a state of emergency, allowing all users to immediately withdraw all their staked tokens;
- set state variables, affecting the pool logic on withdraws and deposits.



Recommendation

The risk describes the current project design and potentially makes iterations to improve in the security operation and level of decentralization, which in most cases cannot be resolved entirely at the present stage. We advise the client to carefully manage the privileged account's private key to avoid any potential risks of being hacked. In

general, we strongly recommend centralized privileges or roles in the protocol be improved via a decentralized mechanism or smart-contract-based accounts with enhanced security practices, e.g., multisignature wallets. Indicatively, here are some feasible suggestions that would also mitigate the potential risk at a different level in terms of short-term, long-term and permanent:

Short Term:

Timelock and Multi sign (⅔, ⅗) combination *mitigate* by delaying the sensitive operation and avoiding a single point of key management failure.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
  AND
- Assignment of privileged roles to multi-signature wallets to prevent a single point of failure due to the private key compromised;
  AND
- A medium/blog link for sharing the timelock contract and multi-signers addresses information with the public audience.

Long Term:

Timelock and DAO, the combination, *mitigate* by applying decentralization and transparency.

- Time-lock with reasonable latency, e.g., 48 hours, for awareness on privileged operations;
  AND
- Introduction of a DAO/governance/voting module to increase transparency and user involvement.
  AND
- A medium/blog link for sharing the timelock contract, multi-signers addresses, and DAO information with the public audience.

Permanent:

Renouncing the ownership or removing the function can be considered *fully resolved*.

- Renounce the ownership and never claim back the privileged roles.
  OR
- Remove the risky functionality.

Alleviation

[Vibranium Audits] : The team acknowledged the finding and decided to remain unchanged.

DISCLAIMER | VIBRANIUM AUDITS

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 Vibranium Audits' 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 Vibranium Audits 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. Vibranium Audits' position is that each company and individual are responsible for their own due diligence and continuous security. Vibranium Audits' 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 Vibranium Audits 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, VIBRANIUM AUDITS HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE SERVICES, ASSESSMENT REPORT, OR OTHER MATERIALS . WITHOUT LIMITING THE FOREGOING, VIBRANIUM AUDITS 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, VIBRANIUM AUDITS 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, VIBRANIUM AUDITS 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 VIBRANIUM AUDITS NOR ANY OF VIBRANIUM AUDITS' 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. VIBRANIUM AUDITS 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 VIBRANIUM AUDITS' 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 VIBRANIUM AUDITS 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 VIBRANIUM AUDITS 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.

Vibranium Audits | Securing the Web3 World

Vibranium Audits is a blockchain security company that was founded in 2021 by professors from the University of Greenwich and cyber-security engineers from ITI Capital. As pioneers in the field, Vibranium Audits utilizes best-in-class Formal Verification and AI technology to secure and monitor blockchains, smart contracts, and Web3 apps.