

Smart Contract Security Audit V1

Token Staking Smart Contract Audit

Jun 26, 2025



<https://saferico.com/>

business@saferico.com

https://t.me/SFI_ANN

—

Table of Contents

Table of Contents

Background

Project Information

Smart Contract Information

Executive Summary

File and Function Level Report

File in Scope:

Issues Checking Status

SWC Attack Analysis

Severity Definitions

Audit Findings

Automatic testing

Testing proves

Inheritance graph

Call graph

Source lines

Risk level

Source units in scope

Capabilities

Unified Modeling Language (UML)

Functions signature

Automatic general report

Conclusion

Disclaimer

Background

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Project Information

- **Platform:** Binance Smart Chain
- **Name:** Token Staking
- **Language :** Solidity
- **Contract Address:** 0x873926b4e1f53ca6ccec0cef07a12d789867c546, 0x98021cf19ac7c2be39c74acc07c17e5796d243fe
- **Code Source:** <https://github.com/TerraDharitri/drt-pREWA/tree/main/contracts>

TokenStaking: Stake pREWA, Earn Rewards

A secure, upgradeable Solidity contract for staking native platform tokens (pREWA) with tiered rewards and emergency features.

Overview

Purpose: Allows users to stake pREWA tokens to earn rewards in the same token

Key Features:

Tiered staking

Multiple staking tiers, varying durations, reward multipliers

Upgradeable

Built with OpenZeppelin's Upgradeable contracts flexibility

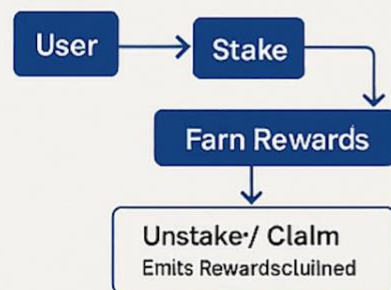
Security

IncluderancyGuaro, Pausable and EmergencyController

Oracle Integration

Optional price feeds

Core Functions



Emergency Withdraw

Penalty Configurable up, MAX_PENALTY

Enabled/disabled by
PARAMETER_ROLE

Usage Flow

Contract Architecture

Base Contracts

Initializable
ReincrencyGuardUpgradable
PausableUpgradable
OwnableUpgradable
TokenStakingStorage
EmergencyAwareBase

Thearanall

EmergenntAurr

AccessControl
EmergencyControffer

External Integrations

- 64dParameterRole
(ondinpaues, page)
- OnlyPauserRole
Controls pause.
- whenNotStakingPaused
Blocks actions when paused

Key Parameters

Modifiers

onlyParameterRole
Resultstis for and settingsclates

onlyPauserRole
Controle pauser or pause.

whenNotStakingPaused
Blocks actions when paused

Emergency Settings

EmergencyController
for diobal pause and shindown



ALERT
imaess, ewergency
witidnoes



CRITICAL
Packes contract

Events

Key Events

Staked
When luges stakes tokens

Unstaked
When htwler, Gunables,,
including servoruice 11

RewardsClaimed
When aoverlon stalled

TierAgded/Updated
When, borore, conodiried

BassAPRUpdated
When APR changes

TokenRecovered
When tokere conover
receToofid

Executive Summary

According to our assessment, the customer's solidity smart contract is **Well-Secured**.

Well Secured	✓
Secured	
Poor Secured	
Insecure	

Automated checks are with remix IDE. All issues were performed by the team, which included the analysis of code functionality, manual audit found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the audit overview section. The general overview is presented in the Project Information section and all issues found are located in the audit overview section.

Team found 0 critical, 0 high, 0 medium, 1 low, 0 very low-level issues and 2 notes in all solidity files of the contract

The files:

TokenStaking.sol

Audit Score:

99% secure



File and Function Level Report

File in Scope:

Contract Name	SHA 256 hash	Contract Address
TokenStaking.sol	4dade80d87703c301e665dca3b4209b20c705238	0x873926b4e1f53ca6ccce0cef07a12d789867c546, 0x98021cf19ac7c2be39c74acc07c17e5796d243fe

- Contract: TokenStaking
- Inherit: Initializable, ReentrancyGuardUpgradeable, PausableUpgradeable, OwnableUpgradeable, TokenStakingStorage, ITokenStaking, EmergencyAwareBase
- Observation: All passed including security check
- Test Report: passed
- Score: passed
- Conclusion: passed

Function	Test Result	Type / Return Type	Score
accessControl	✓	Read / public	Passed
calculateRewards	✓	Read / public	Passed
getBaseAnnualPercentageRate	✓	Read / public	Passed
getEmergencyWithdrawalSettings	✓	Read / public	Passed
getMaxPositionsPerUser	✓	Read / public	Passed
checkEmergencyState	✓	Read / public	Passed
emergencyController	✓	Read / public	Passed
getPositionCount	✓	Read / public	Passed
getStakingPosition	✓	Read / public	Passed
getStakingTokenAddress	✓	Read / public	Passed
getEmergencyController	✓	Read / public	Passed
getTierInfo	✓	Read / public	Passed
isEmergencyPaused	✓	Read / public	Passed

isStakingPaused	✓	Read / public	Passed
oracleIntegration	✓	Read / public	Passed
owner	✓	Read / public	Passed
totalStaked	✓	Read / public	Passed
paused	✓	Read / public	Passed
addTier	✓	Write / public	Passed
renounceOwnership	✓	Write / public	Passed
transferOwnership	✓	Write / public	Passed
claimRewards	✓	Write / public	Passed
initialize	✓	Write / public	Passed
emergencyShutdown	✓	Write / public	Passed
recoverTokens	✓	Write / public	Passed
emergencyWithdraw	✓	Write / public	Passed
pauseStaking	✓	Write / public	Passed
setBaseAnnualPercentageRate	✓	Write / public	Passed
setEmergencyWithdrawal	✓	Write / public	Passed
setEmergencyController	✓	Write / public	Passed
stake	✓	Write / public	Passed
unpauseStake	✓	Write / public	Passed
unstake	✓	Write / public	Passed
updateTier	✓	Write / public	Passed
setMaxPositionsPerUser	✓	Write / public	Passed
setMinStakeDuration	✓	Write / public	Passed
setOracleIntegration	✓	Write / public	Passed

Issues Checking Status

SWC Attack Analysis

The Smart Contract Weakness Classification Registry (SWC Registry) is an implementation of the weakness classification scheme proposed in EIP-1470. It is loosely aligned to the terminologies and structure used in the Common Weakness Enumeration (CWE) for more info check

<https://swcregistry.io/>

No.	Issue Description	Checking Status
136	Unencrypted Private Data On-Chain	Passed
135	Code With No Effects	Passed
134	Message call with hardcoded gas amount	Passed
133	Hash Collisions With Multiple Variable Length Arguments	Passed
132	Unexpected Ether balance	Passed
131	Presence of unused variables	Passed
130	Right-To-Left-Override control character (U+202E)	Passed
129	Typographical Error	Passed
128	DoS with block gas limit.	Passed
127	Arbitrary Jump with Function Type Variable	Passed
126	Insufficient Gas Griefing	Passed
125	Incorrect Inheritance Order	Passed
124	Write to Arbitrary Storage Location	Passed
123	Requirement Violation	Passed
122	Lack of Proper Signature Verification	Passed
121	Missing Protection against Signature Replay Attacks	Passed
120	Weak Sources of Randomness from Chain Attributes	Passed
119	Shadowing State Variables	Passed

118	Incorrect Constructor Name	Passed
117	Signature Malleability	Passed
116	Block values as a proxy for time	Not Passed
115	Authorization through tx.origin	Passed
114	Transaction Order Dependence	Passed
113	DoS with Failed Call	Passed
112	Delegatecall to Untrusted Callee	Passed
111	Use of Deprecated Solidity Functions	Passed
110	Assert Violation	Passed
109	Uninitialized Storage Pointer	Passed
108	State Variable Default Visibility	Passed
107	Reentrancy	Passed
106	Unprotected SELFDESTRUCT Instruction	Passed
105	Unprotected Ether Withdrawal	Passed
104	Unchecked Call Return Value	Passed
103	Floating Pragma	Not Passed
102	Outdated Compiler Version	Passed
101	Integer Overflow and Underflow	Passed
100	Function Default Visibility	Passed

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to tokens loss etc.
High	High-level vulnerabilities are difficult to exploit; however, they also have significant impact on smart contract execution, e.g. public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to tokens lose
Low	Low-level vulnerabilities are mostly related to outdated, unused etc. code snippets, that can't have significant impact on execution
Note	Lowest-level vulnerabilities, code style violations and info statements can't affect smart contract execution and can be ignored.

Audit Findings

Critical:

No Critical severity vulnerabilities were found.

High:

No High severity vulnerabilities were found.

Medium:

No Medium severity vulnerabilities were found.

Low:

#Unused oracleIntegration for Price Feeds

Description

The `oracleIntegration` variable is declared and initialized, but it's not currently used anywhere in the provided `TokenStaking` contract logic (e.g., for calculating dynamic rewards based on external price feeds, or for determining token value).

Recommendation

- If intended for future use: Add a comment explaining its purpose and planned integration points.
- If not needed for this version: Consider removing it and its associated functions (`setOracleIntegration`, `TokenStakingOracleIntegrationSet` event) to reduce contract complexity and gas footprint, and then add it back when its functionality is ready. As it is, it adds complexity without contributing to the current staking logic

Status: **Acknowledged**.

Very Low:

No Very Low severity vulnerabilities were found.

Notes:

#Pragm version not fixed

Description

It is a good practice to lock the solidity version for a live deployment (use 0.8.28 instead of ^0.8.28). contracts should be deployed with the same compiler version and flags that they have been tested the most with. Locking the pragma helps ensure that contracts do not accidentally get deployed using, for example, the latest compiler which may have higher risks of undiscovered bugs. Contracts may also be deployed by

others and the pragma indicates the compiler version intended by the original authors. And avoid Solidity compiler Bugs check here

<https://sepolia.etherscan.io/solcbuginfo>

Remediation

Remove the ^ sign to lock the pragma version.

Use of block.timestamp for comparisons

The value of block.timestamp can be manipulated by the miner. And conditions with strict equality is difficult to achieve - block.timestamp.

```
if ( _lastStakeBlockNumber[msg.sender] >= block.number) revert
LPS_MultiStakeInBlock();
    _lastStakeBlockNumber[msg.sender] = block.number;

    uint256 sTime = block.timestamp;
```

Recommendation

Avoid use of block.timestamp.

Automatic Testing

1- SOLIDITY STATIC ANALYSIS

SOLIDITY STATIC ANALYSIS

☒ Select all ☒ Autorun Run

Security

☒ Select Security

- ☒ **Transaction origin:**
'tx.origin' used
- ☒ **Check-effects-interaction:**
Potential reentrancy bugs
- ☒ **Inline assembly:**
Inline assembly used
- ☒ **Block timestamp:**
Can be influenced by miners
- ☒ **Low level calls:**
Should only be used by experienced devs
- ☒ **Block hash:**
Can be influenced by miners
- ☒ **Selfdestruct:**
Contracts using destructured contract can be broken

Gas & Economy

☒ Select Gas & Economy

- ☒ **Gas costs:**
Too high gas requirement of functions
- ☒ **This on local calls:**
Invocation of local functions via 'this'
- ☒ **Delete dynamic array:**
Use require/assert to ensure complete deletion
- ☒ **For loop over dynamic array:**
Iterations depend on dynamic array's size
- ☒ **Ether transfer in loop:**
Transferring Ether in a for/while/do-while loop

SOLIDITY STATIC ANALYSIS

ERC

☒ Select ERC

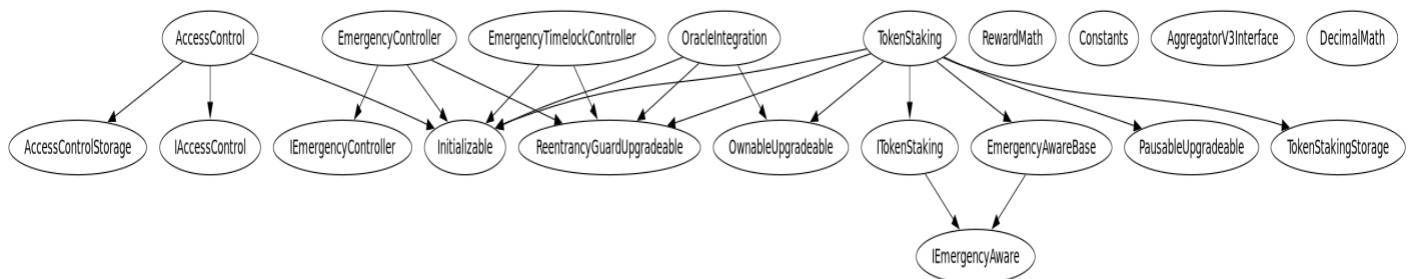
- ☒ **ERC20:**
'decimals' should be 'uint8'

Miscellaneous

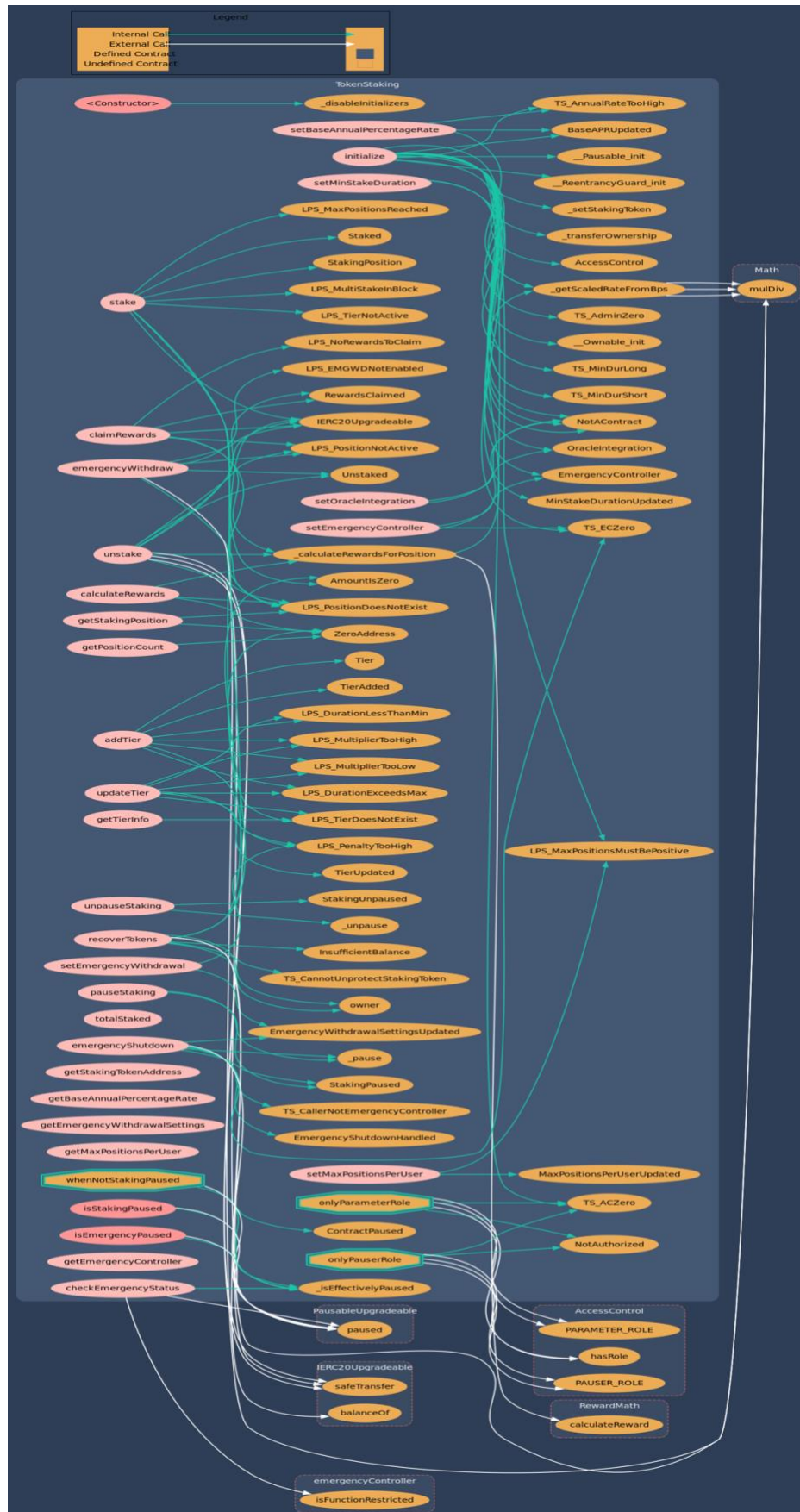
☒ Select Miscellaneous

- ☒ **Constant/View/Pure functions:**
Potentially constant/view/pure functions
- ☒ **Similar variable names:**
Variable names are too similar
- ☒ **No return:**
Function with 'returns' not returning
- ☒ **Guard conditions:**
Ensure appropriate use of require/assert
- ☒ **Result not used:**
The result of an operation not used
- ☒ **String length:**
Bytes length != String length
- ☒ **Delete from dynamic array:**
'delete' leaves a gap in array
- ☒ **Data truncated:**
Division on int/uint values truncates the result

2- Inheritance graph



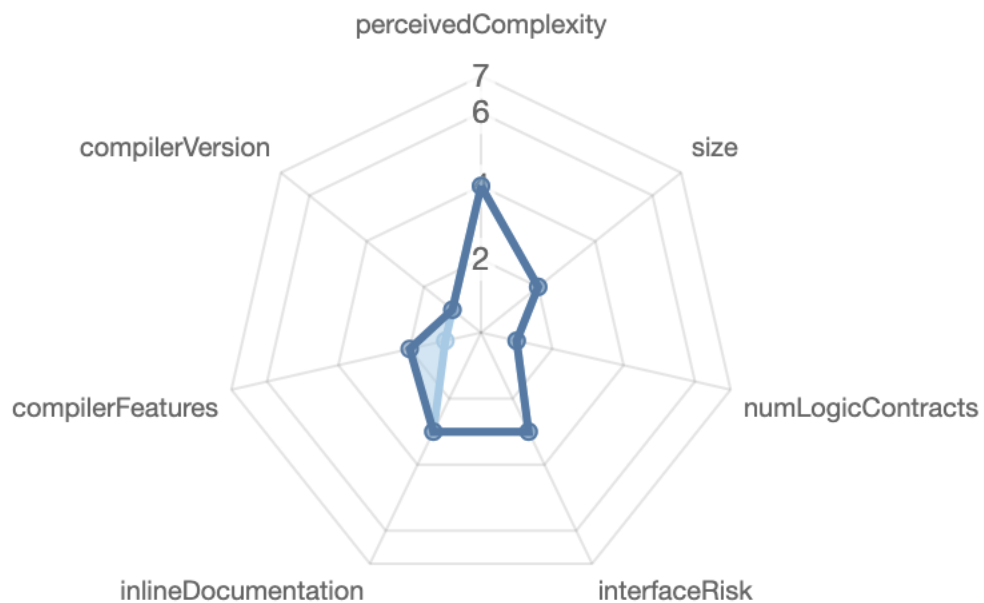
3- Call graph



Source lines



Risk level



Source units in scope

Source Units in Scope

Source Units Analyzed: 1
Source Units in Scope: 1 (100%)

Type	File	Logic Contracts	Interfaces	Lines	nLines	nSLOC	Comment Lines	Complex. Score	Capabilities
	contracts/core/TokenStaking.sol	1	————	639	620	384	155	378	
	Totals	1	————	639	620	384	155	378	

Legend: [—]

- **Lines**: total lines of the source unit
- **nLines**: normalized lines of the source unit (e.g. normalizes functions spanning multiple lines)
- **nSLOC**: normalized source lines of code (only source-code lines; no comments, no blank lines)
- **Comment Lines**: lines containing single or block comments
- **Complexity Score**: a custom complexity score derived from code statements that are known to introduce code complexity (branches, loops, calls, external interfaces, ...)

Capabilities

Components

 Contracts	 Libraries	 Interfaces	 Abstract
1	0	0	0

Exposed Functions

This section lists functions that are explicitly declared public or payable. Please note that getter methods for public stateVars are not included.

 Public	 Payable
30	0

External	Internal	Private	Pure	View
28	22	0	1	14

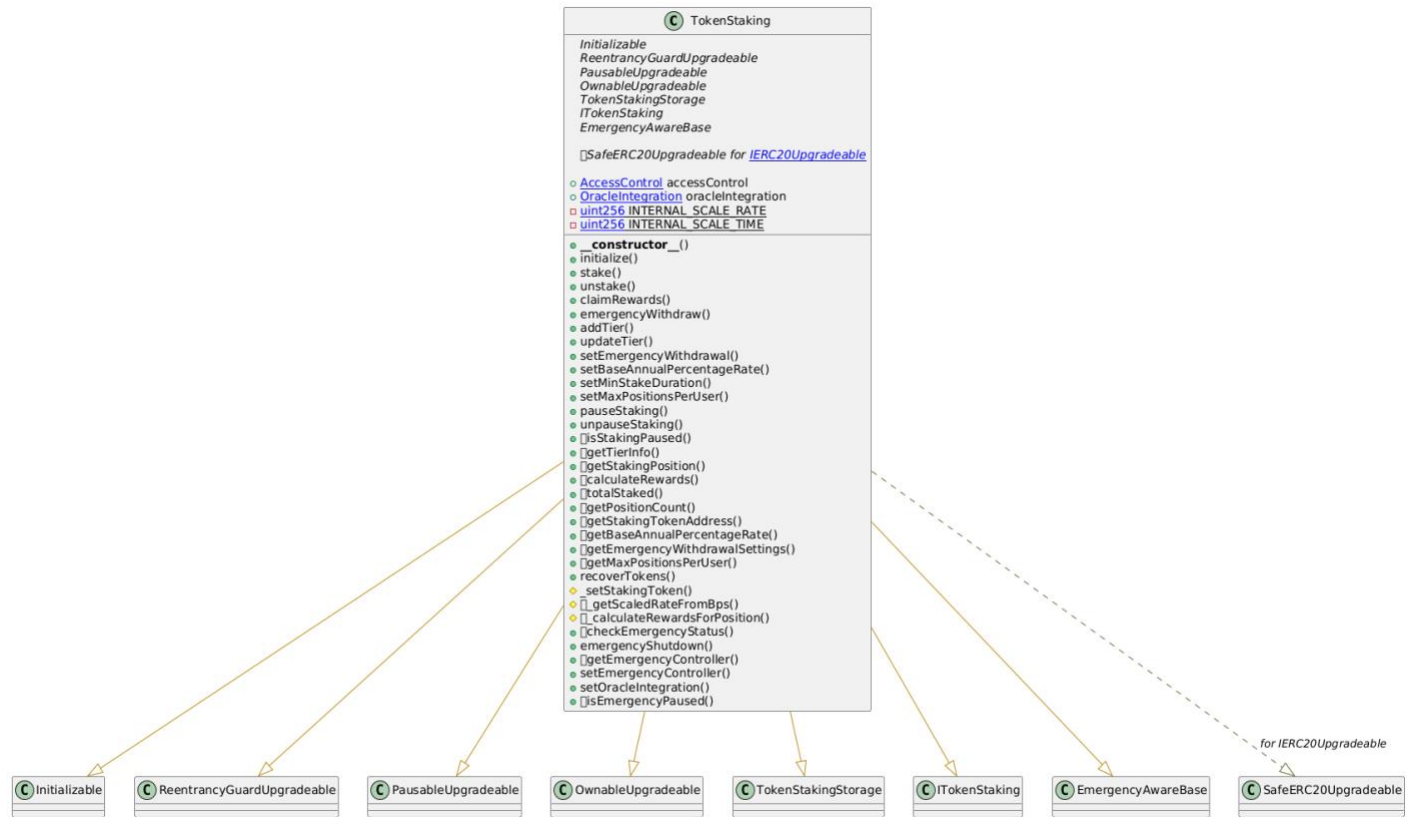
StateVariables

Total	 Public
4	2

Capabilities

Solidity Versions observed	 Experimental Features	 Can Receive Funds	 Uses Assembly	 Has Destroyable Contracts	
0.8.28			yes (5 asm blocks)		
 Transfers ETH	 Low-Level Calls	 DelegateCall	 Uses Hash Functions	 ECRrecover	 New/Create/Create2

Unified Modeling Language (UML)



Functions signature

Function Name	Sighash	Function Signature
-----	-----	-----
initialize	ef335a63	initialize(address,address,address,address,uint256,uint256,address,uint256)
stake	7b0472f0	stake(uint256,uint256)
unstake	2e17de78	unstake(uint256)
claimRewards	0962ef79	claimRewards(uint256)
emergencyWithdraw	5312ea8e	emergencyWithdraw(uint256)
addTier	6358ec57	addTier(uint256,uint256,uint256)
updateTier	6edb9e3c	updateTier(uint256,uint256,uint256,uint256,bool)
setEmergencyWithdrawal	40fd9c15	setEmergencyWithdrawal(bool,uint256)
setBaseAnnualPercentageRate	40d5ee36	setBaseAnnualPercentageRate(uint256)
setMinStakeDuration	aafc5d47	setMinStakeDuration(uint256)
setMaxPositionsPerUser	7a36842d	setMaxPositionsPerUser(uint256)
pauseStaking	f999c506	pauseStaking()
unpauseStaking	93f4bcde	unpauseStaking()
isStakingPaused	1ea7ca89	isStakingPaused()
getTierInfo	cc9d7519	getTierInfo(uint256)
getStakingPosition	e455aea5	getStakingPosition(address,uint256)
calculateRewards	beb8314c	calculateRewards(address,uint256)
totalStaked	817b1cd2	totalStaked()
getPositionCount	0234b445	getPositionCount(address)
getStakingTokenAddress	5ele09a1	getStakingTokenAddress()
getBaseAnnualPercentageRate	294558ab	getBaseAnnualPercentageRate()
getEmergencyWithdrawalSettings	95bc252c	getEmergencyWithdrawalSettings()
getMaxPositionsPerUser	b8e374a0	getMaxPositionsPerUser()
recoverTokens	069c9fae	recoverTokens(address,uint256)
checkEmergencyStatus	8aed668a	checkEmergencyStatus(bytes4)
emergencyShutdown	eb1676c1	emergencyShutdown(uint8)
getEmergencyController	c993cc9d	getEmergencyController()
setEmergencyController	6ca7dc89	setEmergencyController(address)
setOracleIntegration	a9361199	setOracleIntegration(address)
isEmergencyPaused	290d10c4	isEmergencyPaused()

Automatic general report

Files Description Table

File Name	SHA-1 Hash
/Users/macbook/Desktop/drt-pREWA/contracts/core/TokenStaking.sol	4dade80d87703c301e665dca3b4209b20c705238
/Users/macbook/Desktop/drt-pREWA/contracts/core/storage/TokenStakingStorage.sol	26fa66b8f048ee31baad1f88581721dd4a7844c8
/Users/macbook/Desktop/drt-pREWA/contracts/core/interfaces/ITokenStaking.sol	da44791718da6b54ecb51e4f84ec6202f27352f9
/Users/macbook/Desktop/drt-pREWA/contracts/interfaces/IEmergencyAware.sol	be6e0a371b0a5f62d5c7dc06e5c0c4121dcc7ca1
/Users/macbook/Desktop/drt-pREWA/contracts/libraries/RewardMath.sol	364dab3e9f83972a6b43d70f4c87cbf95548b475
/Users/macbook/Desktop/drt-pREWA/contracts/libraries/Constants.sol	62835a8af9d7ab21c0cad9ca03abff6cf4e8e68f
/Users/macbook/Desktop/drt-pREWA/contracts/controllers/EmergencyController.sol	8e73765eaa98f95db8f5eb7a40cd13b0dc845266
/Users/macbook/Desktop/drt-pREWA/contracts/access/AccessControl.sol	40163fa249f10365c03cf1fa9ddd26e2f6eb1005
/Users/macbook/Desktop/drt-pREWA/contracts/access/storage/AccessControlStorage.sol	2a1f4c3d6956a89011b090a62b15254b1d720d65
/Users/macbook/Desktop/drt-pREWA/contracts/access/interfaces/IAccessControl.sol	540ec54eaadelc05a650af086ebf959654ec6322
/Users/macbook/Desktop/drt-pREWA/contracts/libraries/Errors.sol	0974f6f49e3b655fa93a2792154f1b506ec03c74
/Users/macbook/Desktop/drt-pREWA/contracts/interfaces/IEmergencyController.sol	40bc149ec8a1da85c0e4c6170b06f3a0f3b77f3b
/Users/macbook/Desktop/drt-pREWA/contracts/controllers/EmergencyTimelockController.sol	94735e88ad7f750ead488b7ad618b1486cbdb483
/Users/macbook/Desktop/drt-pREWA/contracts/oracle/OracleIntegration.sol	56835e91c3d168cbc4e565e742c575c2117bb3bb
/Users/macbook/Desktop/drt-pREWA/contracts/interfaces/AggregatorV3Interface.sol	008fa0a63980b32bdecef492c7da1ae5b441a5c3
/Users/macbook/Desktop/drt-pREWA/contracts/libraries/DecimalMath.sol	1f5b0a2a73498dc5cb877c08aea3c971646fb4a5
/Users/macbook/Desktop/drt-pREWA/contracts/utils/EmergencyAwareBase.sol	528be04847c5d3cf03edd961c878359eb3cafc6a

Contracts Description Table

Contract	Type	Bases	
:-----:-----:-----:-----			
L	**Function Name**	**Visibility**	**Mutability**
Modifiers			
TokenStaking Implementation Initializable, ReentrancyGuardUpgradeable, PausableUpgradeable, OwnableUpgradeable, TokenStakingStorage, ITokenStaking, EmergencyAwareBase			
L <Constructor>	Public !	⊗	NO !
L initialize	External !	⊗	initializer
L stake	External !	⊗	nonReentrant whenNotStakingPaused
L unstake	External !	⊗	nonReentrant
L claimRewards	External !	⊗	nonReentrant
whenNotStakingPaused			
L emergencyWithdraw	External !	⊗	nonReentrant
L addTier	External !	⊗	onlyParameterRole nonReentrant
L updateTier	External !	⊗	onlyParameterRole nonReentrant
L setEmergencyWithdrawal	External !	⊗	onlyParameterRole nonReentrant
L setBaseAnnualPercentageRate	External !	⊗	onlyParameterRole nonReentrant
L setMinStakeDuration	External !	⊗	onlyParameterRole nonReentrant
L setMaxPositionsPerUser	External !	⊗	onlyParameterRole nonReentrant
L pauseStaking	External !	⊗	onlyPauserRole nonReentrant
L unpauseStaking	External !	⊗	onlyPauserRole nonReentrant
L isStakingPaused	Public !		NO !
L getTierInfo	External !		NO !
L getStakingPosition	External !		NO !
L calculateRewards	External !		NO !
L totalStaked	External !		NO !
L getPositionCount	External !		NO !
L getStakingTokenAddress	External !		NO !
L getBaseAnnualPercentageRate	External !		NO !
L getEmergencyWithdrawalSettings	External !		NO !
L getMaxPositionsPerUser	External !		NO !
L recoverTokens	External !	⊗	onlyOwner nonReentrant
L _setStakingToken	Internal 🔒	⊗	
L _getScaledRateFromBps	Internal 🔒		
L _calculateRewardsForPosition	Internal 🔒		
L checkEmergencyStatus	External !		NO !
L emergencyShutdown	External !	⊗	NO !
L getEmergencyController	External !		NO !
L setEmergencyController	External !	⊗	onlyOwner

```

| L | setOracleIntegration | External ! | 🔒 | onlyOwner |
| L | isEmergencyPaused | Public ! | | NO! |
|||||
| **TokenStakingStorage** | Implementation | |||
|||||
| **ITokenStaking** | Interface | IEmergencyAware |||
| L | initialize | External ! | 🔒 | NO! |
| L | stake | External ! | 🔒 | NO! |
| L | unstake | External ! | 🔒 | NO! |
| L | claimRewards | External ! | 🔒 | NO! |
| L | emergencyWithdraw | External ! | 🔒 | NO! |
| L | addTier | External ! | 🔒 | NO! |
| L | updateTier | External ! | 🔒 | NO! |
| L | setEmergencyWithdrawal | External ! | 🔒 | NO! |
| L | setBaseAnnualPercentageRate | External ! | 🔒 | NO! |
| L | setMinStakeDuration | External ! | 🔒 | NO! |
| L | setMaxPositionsPerUser | External ! | 🔒 | NO! |
| L | pauseStaking | External ! | 🔒 | NO! |
| L | unpauseStaking | External ! | 🔒 | NO! |
| L | isStakingPaused | External ! | | NO! |
| L | getTierInfo | External ! | | NO! |
| L | getStakingPosition | External ! | | NO! |
| L | calculateRewards | External ! | | NO! |
| L | totalStaked | External ! | | NO! |
| L | getPositionCount | External ! | | NO! |
| L | getStakingTokenAddress | External ! | | NO! |
| L | getBaseAnnualPercentageRate | External ! | | NO! |
| L | getEmergencyWithdrawalSettings | External ! | | NO! |
| L | getMaxPositionsPerUser | External ! | | NO! |
|||||
| **IEmergencyAware** | Interface | |||
| L | checkEmergencyStatus | External ! | | NO! |
| L | emergencyShutdown | External ! | 🔒 | NO! |
| L | getEmergencyController | External ! | | NO! |
| L | setEmergencyController | External ! | 🔒 | NO! |
| L | isEmergencyPaused | External ! | | NO! |
|||||
| **RewardMath** | Library | |||
| L | calculateReward | Internal 🔒 | | |
| L | calculateAPR | Internal 🔒 | | |
|||||
| **Constants** | Library | |||
|||||
| **EmergencyController** | Implementation | Initializable,
ReentrancyGuardUpgradeable, IEmergencyController |||
| L | <Constructor> | Public ! | 🔒 | NO! |
| L | initialize | External ! | 🔒 | initializer |
| L | setRequiredApprovals | External ! | 🔒 | onlyAdminRole |
| L | setLevel3TimelockDuration | External ! | 🔒 | onlyAdminRole |
| L | setRecoveryAdminAddress | External ! | 🔒 | onlyAdminRole |

```

```
| L | approveLevel3Emergency | External ! | 🔒 | onlyEmergencyRole  
nonReentrant |  
| L | cancelLevel3Emergency | External ! | 🔒 | onlyEmergencyRole  
nonReentrant |  
| L | executeLevel3Emergency | External ! | 🔒 | onlyEmergencyRole  
nonReentrant |  
| L | setEmergencyLevel | External ! | 🔒 | onlyEmergencyRole  
nonReentrant |  
| L | enableEmergencyWithdrawal | External ! | 🔒 | onlyEmergencyRole  
nonReentrant |  
| L | pauseSystem | External ! | 🔒 | onlyPauserRole nonReentrant |  
| L | unpauseSystem | External ! | 🔒 | onlyPauserRole nonReentrant |  
| L | recoverTokens | External ! | 🔒 | onlyEmergencyRole nonReentrant |  
|  
| L | registerEmergencyAwareContract | External ! | 🔒 |  
onlyEmergencyRole |  
| L | removeEmergencyAwareContract | External ! | 🔒 |  
onlyEmergencyRole |  
| L | processEmergencyForContract | External ! | 🔒 | nonReentrant |  
| L | updateFunctionRestriction | External ! | 🔒 | onlyEmergencyRole |  
| L | getEmergencyLevel | External ! | |NO! |  
| L | getEmergencyWithdrawalSettings | External ! | |NO! |  
| L | isSystemPaused | External ! | |NO! |  
| L | getEmergencyAwareContractsPaginated | External ! | |NO! |  
| L | getApprovalStatus | External ! | |NO! |  
| L | isFunctionRestricted | External ! | |NO! |  
| L | _resetApprovals | Internal 🗝️ | 🔒 | |  
||||||  
| **AccessControl** | Implementation | Initializable,  
AccessControlStorage, IAccessControl |||  
| L | <Constructor> | Public ! | 🔒 |NO! |  
| L | initialize | External ! | 🔒 | initializer |  
| L | hasRole | External ! | |NO! |  
| L | getRoleAdmin | External ! | |NO! |  
| L | grantRole | External ! | 🔒 |NO! |  
| L | revokeRole | External ! | 🔒 |NO! |  
| L | renounceRole | External ! | 🔒 |NO! |  
| L | setRoleAdmin | External ! | 🔒 |NO! |  
| L | getRoleMember | External ! | |NO! |  
| L | getRoleMemberCount | External ! | |NO! |  
| L | getRoleMembersPaginated | External ! | |NO! |  
| L | _grantRole | Internal 🗝️ | 🔒 | |  
| L | _revokeRole | Internal 🗝️ | 🔒 | |  
| L | _setRoleAdmin | Internal 🗝️ | 🔒 | |  
||||||  
| **AccessControlStorage** | Implementation | |||  
||||||  
| **IAccessControl** | Interface | |||  
| L | hasRole | External ! | |NO! |  
| L | getRoleAdmin | External ! | |NO! |  
| L | grantRole | External ! | 🔒 |NO! |
```

```

| L | revokeRole | External ! |  |NO! |
| L | renounceRole | External ! |  |NO! |
| L | getRoleMember | External ! |  |NO! |
| L | getRoleMemberCount | External ! |  |NO! |
| L | getRoleMembersPaginated | External ! |  |NO! |
|||||
| **IEmergencyController** | Interface | |||
| L | setEmergencyLevel | External ! |  |NO! |
| L | enableEmergencyWithdrawal | External ! |  |NO! |
| L | pauseSystem | External ! |  |NO! |
| L | unpauseSystem | External ! |  |NO! |
| L | recoverTokens | External ! |  |NO! |
| L | getEmergencyLevel | External ! |  |NO! |
| L | getEmergencyWithdrawalSettings | External ! |  |NO! |
| L | isSystemPaused | External ! |  |NO! |
| L | getEmergencyAwareContractsPaginated | External ! |  |NO! |
|||||
| **EmergencyTimelockController** | Implementation | Initializable,
ReentrancyGuardUpgradeable |||
| L | <Constructor> | Public ! |  |NO! |
| L | initialize | External ! |  | initializer |
| L | setAllowedTarget | External ! |  | onlyEmergencyRole |
| L | setAllowedFunctionSelector | External ! |  | onlyEmergencyRole |
|
| L | proposeEmergencyAction | External ! |  | onlyEmergencyRole
nonReentrant |
| L | executeEmergencyAction | External ! |  | onlyEmergencyRole
nonReentrant |
| L | cancelEmergencyAction | External ! |  | onlyEmergencyRole
nonReentrant |
| L | updateTimelockDuration | External ! |  | onlyEmergencyRole |
| L | getActionStatus | External ! |  |NO! |
| L | getAllActionIds | External ! |  |NO! |
| L | getActionDetails | External ! |  |NO! |
| L | isFunctionSelectorAllowed | External ! |  |NO! |
| L | isTargetAllowed | External ! |  |NO! |
|||||
| **OracleIntegration** | Implementation | Initializable,
OwnableUpgradeable, ReentrancyGuardUpgradeable |||
| L | <Constructor> | Public ! |  |NO! |
| L | initialize | External ! |  | initializer |
| L | setLiquidityManagerAddress | External ! |  | onlyOwner |
| L | setPriceFeed | External ! |  | onlyOwner nonReentrant |
| L | registerLPToken | External ! |  | onlyLiquidityManagerOrOwner
nonReentrant |
| L | setFallbackPrice | External ! |  | onlyOwner nonReentrant |
| L | setStalenessThreshold | External ! |  | onlyOwner nonReentrant |
|
| L | setMinAcceptablePrice | External ! |  | onlyOwner nonReentrant |
|
| L | getTokenPrice | Public ! |  |NO! |

```

L	fetchAndReportTokenPrice	External	!	⬢	nonReentrant	
L	getLPTokenValue	External	!	NO!		
L	getLPTokenValueAlternative	External	!	NO!		
L	validatePriceAgainstOracle	External	!	NO!		
L	_getPriceFromOracle	Private	🔒			
L	_fetchAndReportPriceFromOracle	Private	🔒	⬢		
L	_verifyPriceFeed	Private	🔒			
L	_getPriceFeedDecimals	Private	🔒			
L	convertToStandardPrecision	Public	!	NO!		
L	_getTokenDecimals	Private	🔒			
L	getPriceFeedInfo	External	!	NO!		
L	getLPTokenInfo	External	!	NO!		
L	getStalenessThreshold	External	!	NO!		
L	getMinAcceptablePrice	External	!	NO!		
AggregatorV3Interface		Interface				
L	decimals	External	!	NO!		
L	description	External	!	NO!		
L	version	External	!	NO!		
L	latestRoundData	External	!	NO!		
L	getRoundData	External	!	NO!		
DecimalMath		Library				
L	mulScaled	Internal	🔒			
L	divScaled	Internal	🔒			
L	mulDiv	Internal	🔒			
L	calculatePercentage	Internal	🔒			
L	applySlippage	Internal	🔒			
L	scaleUp	Internal	🔒			
L	scaleDown	Internal	🔒			
L	weightedAverage	Internal	🔒			
L	compound	Internal	🔒			
L	divRounded	Internal	🔒			
EmergencyAwareBase		Implementation		IEmergencyAware		
L	_isEffectivelyPaused	Internal	🔒			

Legend

Symbol	Meaning
⬢	Function can modify state
🔒	Function is payable

Conclusion

The contracts are written systematically. Team found no critical issues. So, it is good to go for production.

Since possible test cases can be unlimited and developer level documentation (code flow diagram with function level description) not provided, for such an extensive smart contract protocol, we provide no such guarantee of future outcomes. We have used all the latest static tools and manual observations to cover maximum possible test cases to scan Everything.

Security state of the reviewed contract is “Well Secured”.

- ✓ No volatile code.
- ✓ No high severity issues were found.

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as of the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against the team on the basis of what it says or doesn't say, or how team produced it, and it is important for you to conduct your own independent investigations before making any decisions. team go into more detail on this in the below disclaimer below – please make sure to read it in full.

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and Saferico and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (Saferico s) owe no duty of care towards you or any other person, nor does Saferico make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and Saferico hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, Saferico hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Saferico, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.