Cyberscope

Audit Report
Staking

October 2024

Network	BSC
Address	0x8461E6429248656e5479B4bd09f918CBc016b8d5
Audited by	© cyberscope

Table of Contents

Risk Classification

The criticality of findings in Cyberscope's smart contract audits is determined by evaluating multiple variables. The two primary variables are:

1. **Likelihood of Exploitation**: This considers how easily an attack can be executed, including the economic feasibility for an attacker.
2. **Impact of Exploitation**: This assesses the potential consequences of an attack, particularly in terms of the loss of funds or disruption to the contract's functionality.

Based on these variables, findings are categorized into the following severity levels:

1. **Critical**: Indicates a vulnerability that is both highly likely to be exploited and can result in significant fund loss or severe disruption. Immediate action is required to address these issues.
2. **Medium**: Refers to vulnerabilities that are either less likely to be exploited or would have a moderate impact if exploited. These issues should be addressed in due course to ensure overall contract security.
3. **Minor**: Involves vulnerabilities that are unlikely to be exploited and would have a minor impact. These findings should still be considered for resolution to maintain best practices in security.
4. **Informative**: Points out potential improvements or informational notes that do not pose an immediate risk. Addressing these can enhance the overall quality and robustness of the contract.

Severity	Likelihood / Impact of Exploitation
Critical	Highly Likely / High Impact
Medium	Less Likely / High Impact or Highly Likely/ Lower Impact
Minor / Informative	Unlikely / Low to no Impact

Review

Explorer	https://bscscan.com/address/0x8461e6429248656e5479b4bd09f918cbc016b8d5

Audit Updates

Initial Audit	29 Oct 2024

Source Files

Filename	SHA256
PaxeStaking.sol	15501ae5b0cafe4fd7e4da51230b769de9e8e4a52357b719c75bac6cbdd5f49e

Overview

Set Rates Function

The `setRates` function allows the contract owner to adjust the reward rates for each staking duration, where the rates are expressed in basis points (1e8 = 100%). Upon setting new rates, it emits an `EarnRatesUpdated` event.

Deposit Function

The `deposit` function enables users to stake a specified amount of PAXE tokens for a chosen lock duration, in exchange for pPAXE reward tokens based on the selected duration's rate. A fixed deposit fee is collected and sent to the treasury. Users can designate a referrer, who may also receive rewards if eligible. The function updates the oracle, transfers PAXE tokens from the user to the contract, calculates and mints pPAXE rewards, and records deposit information for tracking. This function emits a `Deposit` event upon completion.

Withdraw Function

The `withdraw` function allows users to retrieve their staked PAXE tokens once the locking period has ended. It loops through the user's deposits, identifies and unlocks eligible funds, and transfers them back to the user. The function removes expired deposits from storage and emits a `Withdraw` event once the transfer is complete.

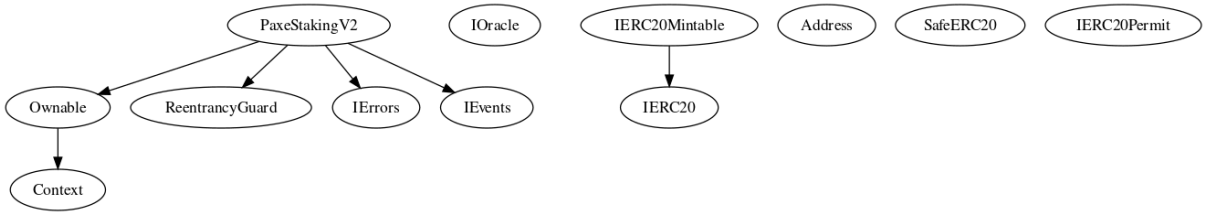
Findings Breakdown

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	0	0	0	0
Medium	0	0	0	0
Minor / Informative	0	0	0	0

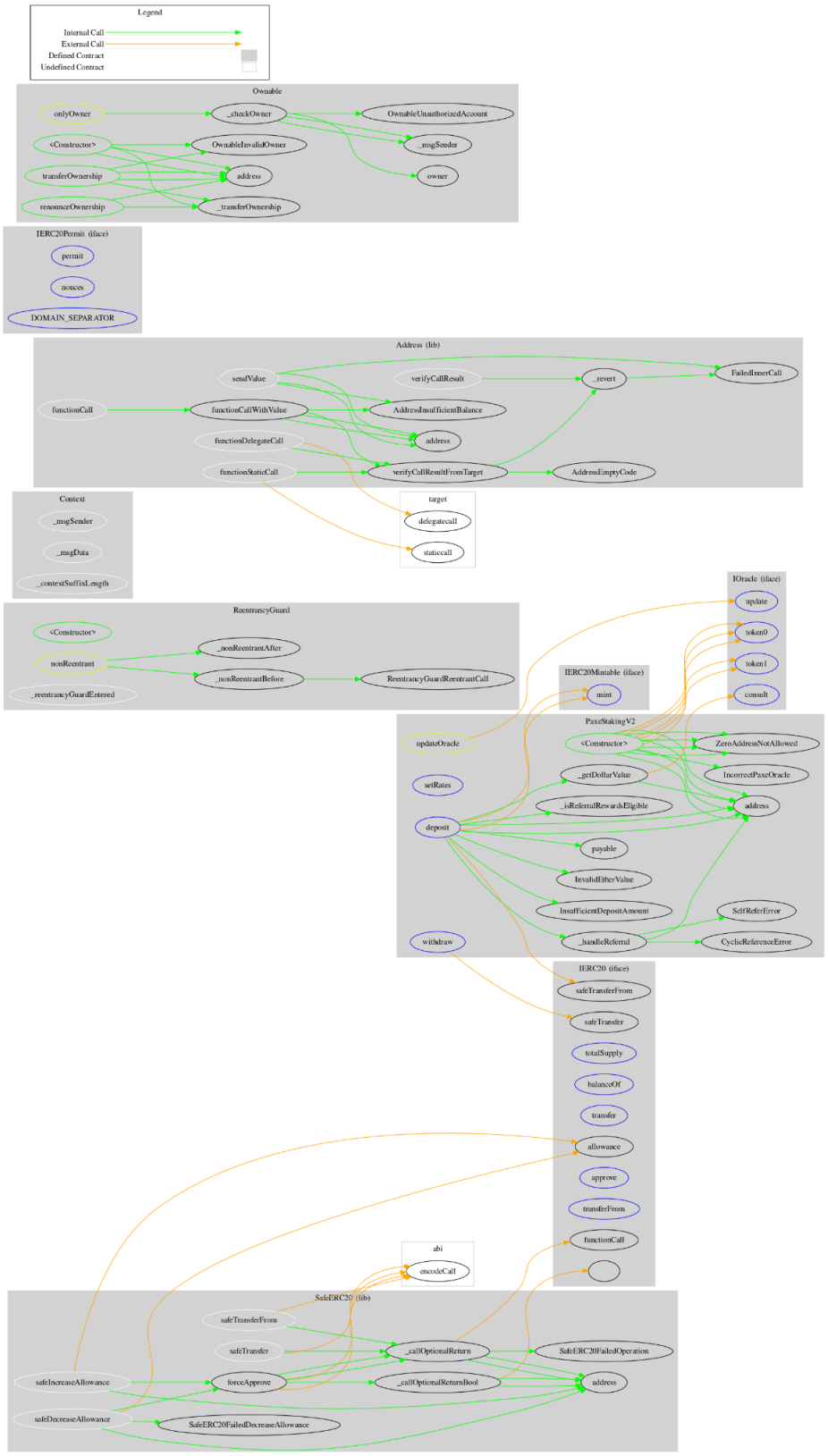
Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
PaxeStaking	Implementation	Ownable, ReentrancyGuard, IErrors, IEvents		
		Public	✓	Ownable
	setRates	External	✓	onlyOwner
	deposit	External	Payable	nonReentrant updateOracle
	withdraw	External	✓	nonReentrant
	_handleReferral	Internal	✓	
	_handleReferralRewards	Internal	✓	
	_checkCyclicReference	Internal		
	_isReferralRewardsEligible	Internal		
	_getDollarValue	Internal		

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
Ownable
onlyOwner
_checkOwner
OwnableUnauthorizedAccount
_msgSender
<Constructor>
OwnableInvalidOwner
owner
transferOwnership
address
renounceOwnership
_transferOwnership
IERC20Permit (iface)
permit
nonces
DOMAIN_SEPARATOR
Address (lib)
sendValue
verifyCallResult
_revert
FailedInnerCall
functionCall
functionCallWithValue
AddressInsufficientBalance
address
functionDelegateCall
functionStaticCall
verifyCallResultFromTarget
AddressEmptyCode
Context
_msgSender
_msgData
_contextSuffixLength
target
delegatecall
staticcall
ReentrancyGuard
<Constructor>
_nonReentrantAfter
nonReentrant
_nonReentrantBefore
ReentrancyGuardReentrantCall
_reentrancyGuardEntered
IOracle (iface)
update
token0
token1
consult
IERC20Mintable (iface)
mint
PaxeStakingV2
updateOracle
<Constructor>
ZeroAddressNotAllowed
IncorrectPaxeOracle
setRates
_getDollarValue
_isReferralRewardsEligible
address
deposit
payable
InvalidEtherValue
InsufficientDepositAmount
SelfReferError
withdraw
_handleReferral
CyclicReferenceError
IERC20 (iface)
safeTransferFrom
safeTransfer
totalSupply
balanceOf
transfer
allowance
approve
transferFrom
functionCall
abi
encodeCall
SafeERC20 (lib)
safeTransferFrom
safeTransfer
_callOptionalReturn
SafeERC20FailedOperation
safeIncreaseAllowance
forceApprove
_callOptionalReturnBool
address
safeDecreaseAllowance
SafeERC20FailedDecreaseAllowance

Summary

Staking implements a staking and locking mechanism that rewards stakers PAXE with pPAXE, while also integrating a referral system. The Smart Contract analysis reported no compiler error or critical issues. This audit investigates security issues, business logic concerns and potential improvements.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. 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 Cyberscope’s prior written consent. 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 regarded as an indication of the economics or value of any “product” or “asset” created by any team or project that contracts Cyberscope to perform a security assessment. This document 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 represents an extensive assessment 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 Cyberscope’s position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope’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 Cyberscope are subject to dependencies and are 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.

About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

The Cyberscope team

cyberscope.io