Cyberscope

Audit Report

Paxe Liquid Restaking

October 2024

Network BSC

Address 0x269e1ceb128ccCD5684BbAFF9906D69eD1e9e9C8

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/0x269e1ceb128cccd5684bbaff9906d69ed1e9e9c8

Audit Updates

Initial Audit	02 Oct 2024

Source Files

Filename	SHA256
PaxeRestaking.sol	419b92645eb3caae545857bb40c897a9493edac2a6034b9161b8693f798edf95

Overview

Restake Function

The `restake` function is the entry point for users who wish to stake their `pPAXE` tokens. When a user calls this function, they provide a staking fee, which is transferred to the treasury. If the fee is not exact or if the user tries to stake zero tokens, the function will revert with relevant errors. Upon successful payment, the contract transfers the specified `pPAXE` tokens. The contract then records the stake details, including the amount staked and the timestamp. After this, the function emits a `Restake` event, which logs the user's staking action for transparency.

Claim Function

The `claim` function allows users to collect their earned rewards based on their staked `pPAXE`. Like the restaking process, this function requires the user to pay a fee (`CLAIM_FEE`), which is transferred to the treasury. The contract then calculates the total rewards the user is entitled to by iterating through their stakes. If a stake has completed its staking period of 180 days, it is deleted from the user's record, and no further rewards can be earned from it. The calculated rewards are then transferred to the user in `PAXE` tokens, provided the contract holds enough tokens to cover the claim. Upon a successful claim, the contract emits a `Claim` event, detailing the amount of rewards distributed and the user's address.

Pending Rewards Calculation

The contract includes a `pendingRewards` view function, which allows users to check the total rewards they are eligible to claim without initiating a claim transaction. This function scans the user's stakes and calculates the rewards they have earned but not yet claimed. It serves as a convenient tool for users to monitor their earnings before deciding to execute a claim.

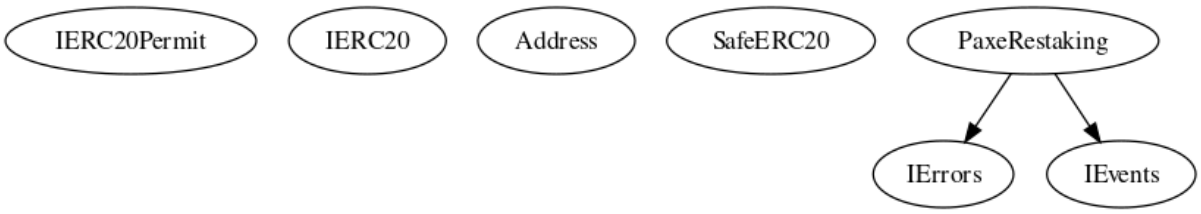
Findings Breakdown

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

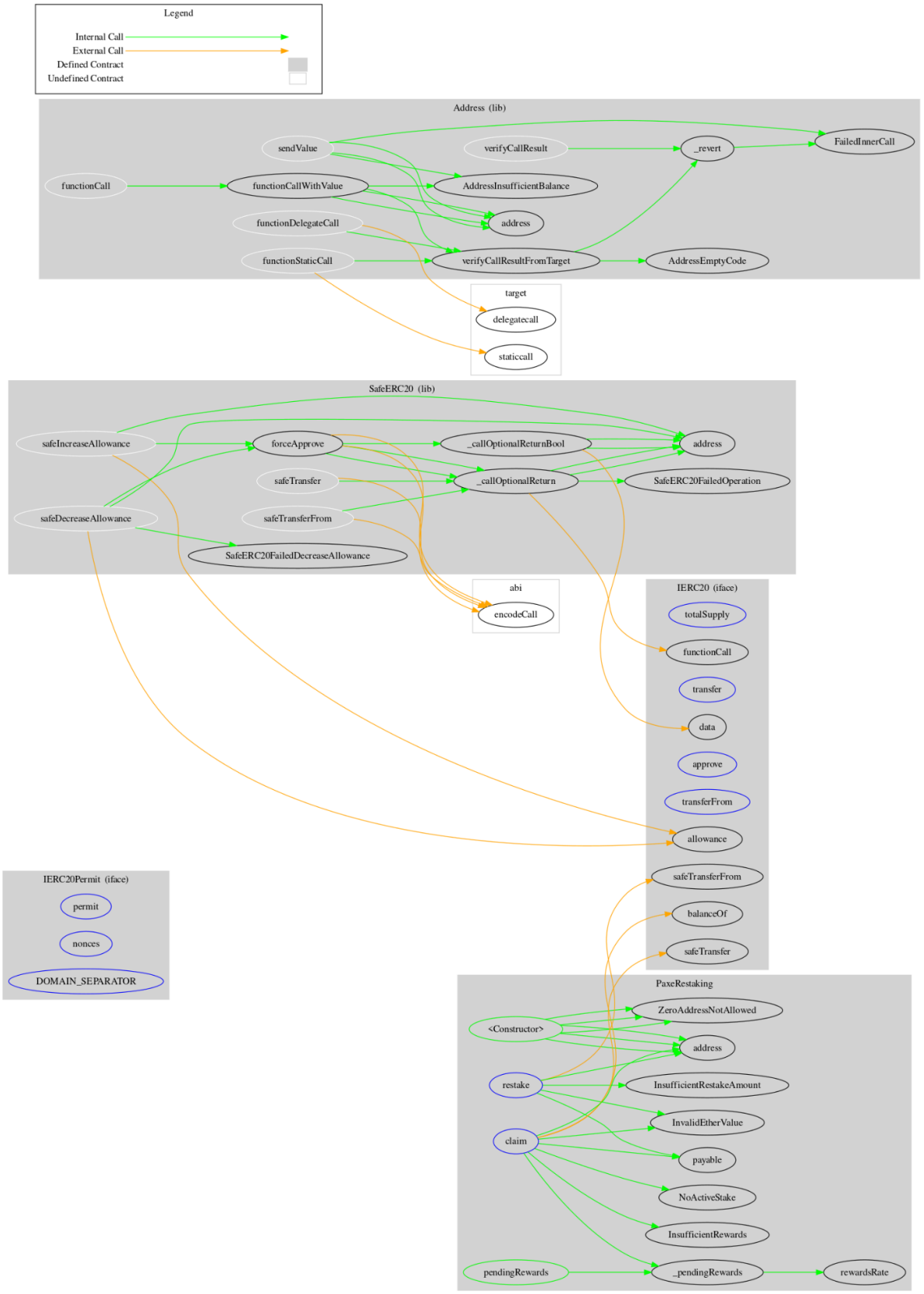
Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
PaxeRestaking	Implementation	IErrors, IEvents		
		Public	✓	-
	restake	External	Payable	-
	claim	External	Payable	-
	pendingRewards	Public		-
	_pendingRewards	Internal		
	rewardsRate	Internal		

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
Address (lib)
sendValue
verifyCallResult
_revert
FailedInnerCall
functionCall
functionCallWithValue
AddressInsufficientBalance
address
functionDelegateCall
functionStaticCall
verifyCallResultFromTarget
AddressEmptyCode
target
delegatecall
staticcall
SafeERC20 (lib)
safeIncreaseAllowance
forceApprove
_callOptionalReturnBool
address
safeTransfer
_callOptionalReturn
SafeERC20FailedOperation
safeDecreaseAllowance
safeTransferFrom
SafeERC20FailedDecreaseAllowance
abi
encodeCall
IERC20 (iface)
totalSupply
functionCall
transfer
data
approve
transferFrom
allowance
safeTransferFrom
balanceOf
safeTransfer
IERC20Permit (iface)
permit
nonces
DOMAIN_SEPARATOR
PaxeRestaking
ZeroAddressNotAllowed
<Constructor>
address
restake
InsufficientRestakeAmount
InvalidEtherValue
claim
payable
NoActiveStake
InsufficientRewards
pendingRewards
_pendingRewards
rewardsRate

Summary

Paxe Liquid Restaking implements a restaking mechanism that rewards stakers of pPAXE. Paxe is an interesting project that has a friendly and growing community. 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