Cyberscope

Audit Report

Paxe Token

June 2024

Network	BSC
Address	0xd2a3eec06719d5ac66248003b5488e02165dd2fa
Audited by	© cyberscope

Analysis

Critical Medium Minor / Informative Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	MT	Mints Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

Table of Contents

Review

Contract Name	Paxe
Compiler Version	v0.8.16+commit.07a7930e
Optimization	200 runs
Explorer	https://bscscan.com/address/0xd2a3eec06719d5ac66248003b5488e02165dd2fa
Address	0xd2a3eec06719d5ac66248003b5488e02165dd2fa
Network	BSC
Symbol	PAXE
Decimals	18
Total Supply	100,000,000
Badge Eligibility	Yes

Audit Updates

Initial Audit	16 May 2024
Corrected Phase 2	21 May 2024
Corrected Phase 3	04 Jun 2024
Corrected Phase 4	25 Jun 2024

Source Files

Filename	SHA256
Paxe.sol	c3d235fa47439728c42a2743af06911489e0bdcdcbf91f2bcf95a2475f855508

Findings Breakdown

Critical	0
Medium	0
Minor / Informative	1

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	0	0	0	0
Medium	0	0	0	0
Minor / Informative	1	0	0	0

RNCT - Redundant Native Currency Transfer

Criticality	Minor / Informative
Location	Paxe.sol#L1333
Status	Unresolved

Description

The contract includes a function named `claimStuckTokens`. This function is designed to transfer either native currency (e.g., Ether) or ERC20 tokens from the contract to the caller (`msg.sender`). However, there is a redundant piece of code that attempts to transfer native currency, despite the contract not being designed to accept Ether. This redundancy could lead to confusion and unnecessary gas consumption.

```
function claimStuckTokens(address token) external onlyOwner {
    require(token != address(this), "Owner cannot claim native tokens");

    if (token == address(0x0)) {
        payable(msg.sender).transfer(address(this).balance);
        return;
    }

    IERC20 ERC20token = IERC20(token);
    uint256 balance = ERC20token.balanceOf(address(this));
    ERC20token.safeTransfer(msg.sender, balance);
}
```

Recommendation

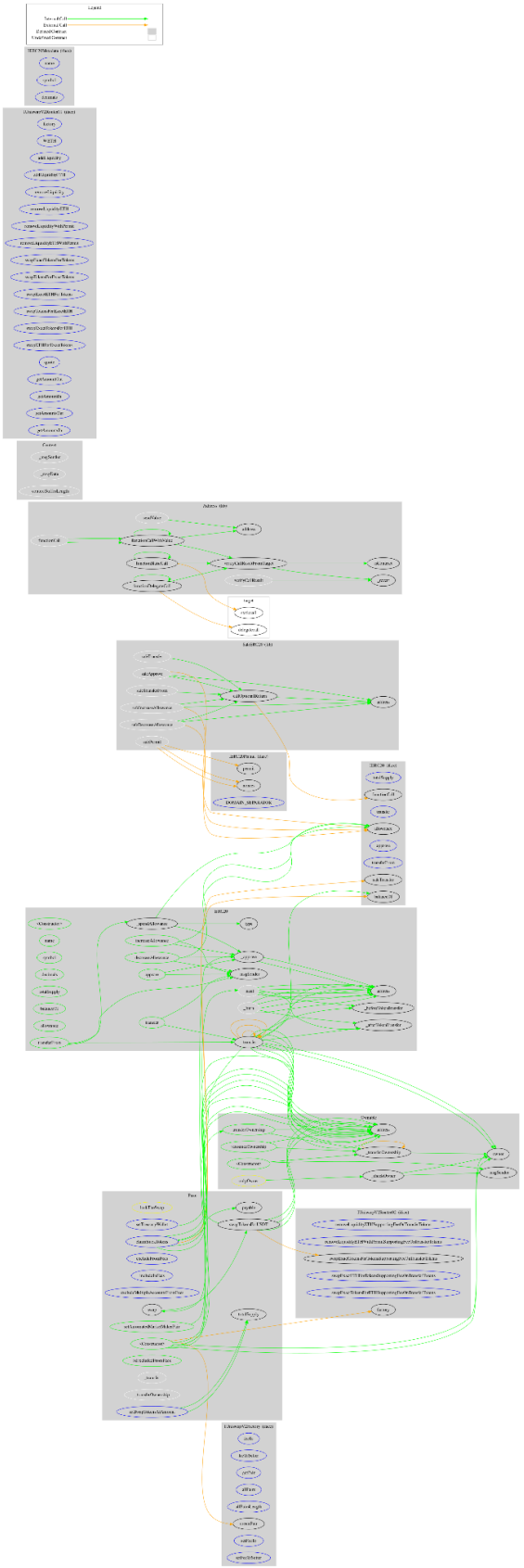
Remove the redundant check and the associated transfer logic for native currency from the `claimStuckTokens` function. The function should only handle the transfer of ERC20 tokens, as this is the intended functionality of the contract. Otherwise, add a `receive` function to the contract.

Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Paxe	Implementation	ERC20, Ownable		
		Public	✓	ERC20
	setSwapTokensAtAmount	External	✓	onlyOwner
	excludeFromFees	External	✓	onlyOwner
	includeInFees	External	✓	onlyOwner
	excludeMultipleAccountsFromFees	External	✓	onlyOwner
	setTreasuryWallet	External	✓	onlyOwner
	claimStuckTokens	External	✓	onlyOwner
	setAutomatedMarketMakerPair	Public	✓	onlyOwner
	isExcludedFromFees	Public		-
	_transfer	Internal	✓	
	_transferOwnership	Internal	✓	
	swap	Private	✓	lockTheSwap
	swapTokensForUSDT	Private	✓	

Inheritance Graph

Flow Graph



Summary

Paxe is an interesting project that has a friendly and growing community. 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

https://www.cyberscope.io