Cyberscope

A TAC Security Company

Audit Report

UnCensored Waves

July 2025

Network : BASE

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

Addresses	0x1A7F059f6Bc234D1D03075B430e26c67856B53dE 0x8fE351FD35DDC08bc2f3c5fA573B44d6E13f97ec 0x885f14Ec5c427767A660174ea0EA8C9953f3549D 0x9c55175284505A184d5e4ab52aA40d68f2253051 0xD29c16A57462EfE0f51A778C3629303e1849bdFE 0x399095b87f77eDD8d811cB69B51db81ca889d315 0xDb51A363bf304e9A0ef66C29496AE5F8F3ABeDA4 0xA2baEcb35ec71EE702Da05a73c8F3F5C4b44F77D
Explorers	https://basescan.org/address/0x1A7F059f6Bc234D1D03075B430e26c67856B53dE https://basescan.org/address/0x8fE351FD35DDC08bc2f3c5fA573B44d6E13f97ec https://basescan.org/address/0x885f14Ec5c427767A660174ea0EA8C9953f3549D https://basescan.org/address/0x9c55175284505A184d5e4ab52aA40d68f2253051 https://basescan.org/address/0xD29c16A57462EfE0f51A778C3629303e1849bdFE https://basescan.org/address/0x399095b87f77eDD8d811cB69B51db81ca889d315 https://basescan.org/address/0xDb51A363bf304e9A0ef66C29496AE5F8F3ABeDA4 https://basescan.org/address/0xA2baEcb35ec71EE702Da05a73c8F3F5C4b44F77D
Network	BASE
Badge Eligibility	Yes

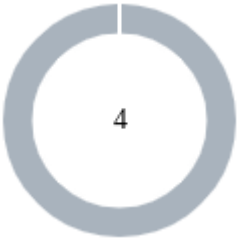
Audit Updates

Initial Audit	06 Jun 2025
Corrected Phase 2	17 Jun 2025
Corrected Phase 3	27 Jun 2025

Source Files

Filename	SHA256
stakingRewards.sol	87874850848cfc952cdc9bee8af1bfeb7aeab3c3f3448a0371c411105cc39ea7
nauy.sol	6d7ddfef4f5d5e848829f83cc5f526a00e43c15a15eec9d5862036ffb12b764e
naun.sol	eab80f3190bac0c9b31a0ad80405a672a7366fe7fbfe06d2b766b569fefe78f4
nau.sol	37676a0efa09a1a5f09c78919bbd90825d179714c0e1d50e46d4d139f0c22938
devTeamVesting.sol	50d9803f2eaedf7b62dca12b515bb8499e951559c1c36d1f4e91793332da4804
controller.sol	66b74b97cfe9d6b5c3c95a901dbbed8d8cef20cf2af343459663a74e408f8fd2

Findings Breakdown



Critical	0
Medium	0
Minor / Informative	4

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	0	0	0	0
Medium	0	0	0	0
Minor / Informative	0	4	0	0

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
●	BT	Burns Tokens	Acknowledged
●	MT	Mints Tokens	Acknowledged
●	PPM	Potential Price Manipulation	Acknowledged
●	TSI	Tokens Sufficiency Insurance	Acknowledged

BT - Burns Tokens

Criticality	Minor / Informative
Location	nau.sol#L104
Status	Acknowledged

Description

The `controller` address has the authority to burn tokens from a specific address. This address may take advantage of it by calling the `burn` function. As a result, the targeted address will lose the corresponding tokens.

```
   function controllerBurn(address account, uint256 amount) external {
        require(msg.sender == controller, "NAU: Not authorized, only
controller can burn");
        _burn(account, amount);
    }
```

Recommendation

The team should carefully manage the private keys of the `controller` account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions.

Temporary Solutions:

These measurements do not decrease the severity of the finding

- Introduce a time-locker mechanism with a reasonable delay.
- Introduce a multi-signature wallet so that many addresses will confirm the action.
- Introduce a governance model where users will vote about the actions.

Permanent Solution:

- Renouncing the ownership, which will eliminate the threats but it is non-reversible.

MT - Mints Tokens

Criticality	Minor / Informative
Location	naun.sol#L29 nauy.sol#L29
Status	Acknowledged

Description

The `controller` address has the authority to mint tokens. This address may take advantage of it by calling the `controllerMint` function. As a result, the contract tokens will be highly inflated.

```
  function controllerMint(address to, uint256 amount) external {
       require(msg.sender == controller, "NAUN: Only controller can mint");
       _mint(to, amount);
   }
```

Recommendation

The team should carefully manage the private keys of the `controller` account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions.

Temporary Solutions:

These measurements do not decrease the severity of the finding

- Introduce a time-locker mechanism with a reasonable delay.
- Introduce a multi-signature wallet so that many addresses will confirm the action.
- Introduce a governance model where users will vote about the actions.

Permanent Solution:

- Renouncing the authority, which will eliminate the threats but it is non-reversible.

PPM - Potential Price Manipulation

Criticality	Minor / Informative
Location	controller.sol#L203
Status	Acknowledged

Description

The contract implements mint and burn operations involving decentralized pools. This design potentially enables price manipulation across different trading pairs to extract value. Such mechanisms are often prone to exploitation, as the token supply depends on the assets in the pool, which in turn are cyclically dependent on the token's price.

```
uint256 amountNAUY = FullMath.mulDiv(valueNAUYInQuote, 1e18, priceNAUY);
uint256 amountNAUN = FullMath.mulDiv(valueNAUNInQuote, 1e18, priceNAUN);
```

Recommendation

The team is advised to refrain from such designs. Instead, it is recommended to leverage the functionalities of the decentralized exchange to perform operations that affect the token supply.

TSI - Tokens Sufficiency Insurance

Criticality	Minor / Informative
Location	devTeamVesting.sol stakingRewards.sol
Status	Acknowledged

Description

The tokens are not held within the contract itself. Instead, the contract is designed to provide the tokens from an external administrator. While external administration can provide flexibility, it introduces a dependency on the administrator's actions, which can lead to various issues and centralization risks.

```
xToken.safeTransfer(devBeneficiary, _amount);
```

```
function fundRewards(uint256 _amount) external onlyRole(FUNDER_ROLE) {
require(_amount > 0, "SR: Cannot fund 0");
// Assumes the FUNDER (msg.sender) has been approved by the source wallet
// or the FUNDER *is* the source wallet and approved this contract.
// Standard: Pull from msg.sender, requires caller to have funds/allowance.
rewardToken.safeTransferFrom(msg.sender, address(this), _amount);
emit RewardsFunded(_amount);
}
```

Recommendation

It is recommended to consider implementing a more decentralized and automated approach for handling the contract tokens. One possible solution is to hold the tokens within the contract itself. If the contract guarantees the process it can enhance its reliability, security, and participant trust, ultimately leading to a more successful and efficient process.

Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
StakingRewards	Implementation	AccessControl, ReentrancyGuard		
		Public	✓	-
	_lastTimeRewardApplicable	Internal		
	rewardPerToken	Public		-
	earned	Public		-
	stake	External	✓	nonReentrant updateReward
	unstake	Public	✓	nonReentrant updateReward
	claimRewards	Public	✓	nonReentrant updateReward
	setRewardRate	External	✓	onlyRole
	fundRewards	External	✓	onlyRole
	recoverExcessRewardTokens	External	✓	onlyRole
NAUY	Implementation	ERC20, AccessControl		
		Public	✓	ERC20
	_update	Internal	✓	
	controllerMint	External	✓	-
	renounceAdmin	External	✓	-

NAUN	Implementation	ERC20, AccessControl		
		Public	✓	ERC20
	_update	Internal	✓	
	controllerMint	External	✓	-
	renounceAdmin	External	✓	-
NAU	Implementation	ERC20, AccessControl		
		Public	✓	ERC20
	setLpPair	External	✓	onlyRole
	setIsExcludedFromMaxWallet	External	✓	onlyRole
	setIsExcludedFromMaxTx	External	✓	onlyRole
	_update	Internal	✓	
	controllerBurn	External	✓	-
	renounceAdmin	External	✓	-
DevTeamVesting	Implementation			
		Public	✓	-
	vestedAmount	Public		-
	claimVestedTokens	External	✓	-
	claimableAmount	Public		-
INAU	Interface	IERC20		
	controllerBurn	External	✓	-

INAUXMintable	Interface	IERC20		
	controllerMint	External	✓	-
Controller	Implementation	AccessControl		
		Public	✓	-
	setTokenAddresses	External	✓	onlyRole
	setQuoteToken	External	✓	onlyRole
	setPool	External	✓	onlyRole
	setTwapInterval	External	✓	onlyRole
	setMaxDataStalePeriod	External	✓	onlyRole
	setL2SequencerOracle	External	✓	onlyRole
	getTwapPrice	Public		-
	transformX	External	✓	-
	renounceAdmin	External	✓	-

Summary

UnCensored Waves contracts implement a token, staking and vesting mechanism. 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.

A **TAC Security** Company

The Cyberscope team

cyberscope.io