CRYPTO CRAT

SMART CONTRACT AUDIT

Bitsniper Staking

Conclusion

The project team of Bitsniper (Bullet) TToken has applied for security auditing of the Smart Contract (0x4358c9A9C27Af7608C3287D1Ebb7cb18DAec5644) they use for Bitsniper staking pools

After detailed test process and examination performed by our expert team, we declare that Smart Contract is successfully PASSED the security audit

Summary

Audit Summary

Audit Result	✓ Passed
KYC Verification	NA
Token Name	Bitsniper Token
Token Symbol	Bullet
Contract Address	0x4358c9A9C27Af7608C3287D1Ebb7cb18DAec5644
Contract Type	Staking Contract
Audited CodeBase	BitsniperStaking.sol
Testnet Address Link	https://testnet.bscscan.com/address/0x3f6d2fD796990b1F797d6DaD4BFb64326c3e1a7D https://testnet.bscscan.com/address/0x0bb36bb2dace92bde2fe502a741e2cd7893eb3a8
Ownership Status	Actively Owned
DApp Link	**https://bitsniper-staking.netlify.app/**
Active Pool Count	4
Application Test	✓ Passed
Wallet Connect Test	✓ Passed
Active Pool's Analyse	✓ Passed
Attack Test	✓ Passed
Emergency Withdraw Fee	25%

- ✓ Based on our comprehensive review and testing, we can confidently state that the mentioned contract has undergone rigorous evaluation and has successfully passed all security tests. The contract exhibits a high level of security against various types of attacks, including but not limited to reentrancy attacks, integer overflows, and unauthorized access attempts. It is important to note that, while the contract has been deemed secure based on the current audit, the rapidly evolving nature of the blockchain ecosystem necessitates regular updates and ongoing security monitoring to address any emerging threats.

Summary of Owner's Privileges

Privilege Description	INFO	LOW	MEDIUM	HIGH
renounceOwnership	✓			
transferOwnership	✓			
claimStuckTokens			●	
addPool	✓			
setFees _ (max 30%)		✓		

* Only privileges which can be controlled by owner and might have potential to effect profit/loss of investors are listed

- To maintain the necessary functionality of the smart contract, the owner has privileges that are necessary but potentially harmful to investors. However, in emergencies, it is recommended that property management be entrusted to an authorized securities company to protect investors' funds and ensure that these privileges are used responsibly. By doing this, the risks associated with the owner's privileges can be reduced by providing an additional layer of protection and increasing the overall security and reliability of the contract.

Summary of Manual Analysis

- During our manual analysis of the smart contract, we identified a crucial aspect related to the ownership privileges. It was observed that the owner must deposit tokens to enable the granting of rewards corresponding to the staked amounts by investors. This ensures the proper functioning of the contract and the equitable distribution of rewards based on the investors' stakes. It is essential to carefully manage this process to maintain transparency and fairness within the contract ecosystem.

Summary of SWC Analysis

✓ The provided source code of the smart contract has undergone a successful SWC (Smart Contract Weakness Classification) analysis, verifying that it adheres to recommended security practices and does not contain common vulnerabilities.

CRYPTO CRAT AUDIT

Table of Contents

CRYPTO CRAT AUDIT

Report Data

This report has been prepared by Cryptocrat experts based on detailed examination of Bitsniper Staking Smart Contract on June 11, 2023.

Audit process performed carefully using Static Analysis and Manual review Techniques as well as Automated test procedures.

The auditing process focuses to the following considerations with collaboration of an expert team

- Functionality test of the Smart Contract to determine if proper logic has been followed throughout the whole process.
- Manually detailed examination of the code line by line by experts.
- Live test by multiple clients using Testnet.
- Analysing failure preparations to check how the Smart Contract performs in case of any bugs and vulnerabilities.
- Checking whether all the libraries used in the code are on the latest version.
- Analysing the security of the on-chain data.

Project Info

Contract Name	**Bitsniper Staking**
Contract	0x4358c9A9C27Af7608C3287D1Ebb7cb18DAec5644
Link to Contract	https://bscscan.com/address/0x4358c9a9c27af7608c3287d1ebb7cb18daec5644
Contract Status	Not verified for security reasons
Platform	Binance Smart Chain
Language	Solidity
Project Web Site	https://bitsniper.io/
DApp Link	https://bitsniper-staking.netlify.app/
Telegram Group	https://t.me/bitsnipergame

OVERVIEW

This Audit Report mainly focuses on overall security of the smart contract. Cryptocrat team scanned the contract and assessed overall system architecture and the smart contract codebase against vulnerabilities, exploitations, hacks, and back-doors to ensure its reliability and correctness.

Auditing Approach and Applied Methodologies

Cryptocrat team has performed rigorous test procedures of the project

- Code design patterns analysis in which smart contract architecture is reviewed to ensure it is structured according to industry standards and safe use of third-party smart contracts and libraries.
- Line-by-line inspection of the Smart Contract to find any potential vulnerability like race conditions, transaction-ordering dependence, timestamp dependence, and denial of service attacks.
- Unit testing Phase, we coded/conducted custom unit tests written for each function in the contract to verify that each function works as expected.
- Automated Test performed with our in-house developed tools to identify vulnerabilities and security flaws of the Smart Contract.

The focus of the audit was to verify that the Smart Contract System is secure, resilient, and working according to the specifications. The audit activities can be grouped in the following three categories:

Security

Identifying security related issues within each contract and the system of contract.

Sound Architecture

Evaluation of the architecture of this system through the lens of established smart contract best practices and general software best practices.

Code Correctness and Quality

A full review of the contract source code. The primary areas of focus include:

- Accuracy
- Readability
- Sections of code with high complexity
- Quantity and quality of test coverage

Risk Classification

SEVERITY	EXPLANATION
INFORMATIONAL	Informational risks are classified as low-impact issues that do not pose an immediate threat to the security or functionality of the smart contract. These risks typically include suggestions for code optimization, improvements in documentation, or best practices that can enhance the overall quality and maintainability of the contract. While not critical, addressing these informational risks is recommended to further strengthen the contract's security posture.
LOW	Low-risk vulnerabilities are minor issues that may have limited impact on the contract's security. These risks are typically related to non-critical code flaws or deviations from best practices that could potentially be exploited under certain circumstances. While the impact is relatively low, it is still advisable to address these vulnerabilities to reduce any potential security risks and ensure the contract operates as intended.
MEDIUM	Medium-risk vulnerabilities pose a moderate level of risk to the security and functionality of the smart contract. These risks may include code vulnerabilities that could potentially be exploited, but with certain constraints or prerequisites. Addressing medium-risk vulnerabilities is crucial to prevent potential security breaches or unintended behaviour that could impact the contract or its users.
HIGH	High-risk vulnerabilities are critical issues that pose significant threats to the security and functionality of the smart contract. These risks typically involve severe code vulnerabilities that can be exploited to manipulate or compromise the contract's behavior, resulting in financial loss or unauthorized access. Immediate attention and remediation of high-risk vulnerabilities are necessary to ensure the contract's integrity and protect the funds and assets associated with it.

It is important to note that risk classification may vary based on the specific audit methodology or framework used, and the assigned risk level should be interpreted in the context of the smart contract being audited.

Disclaimer

This document has been prepared by Cryptocrat solely for the use of the investors to whom it is addressed and for no other purpose. The information contained in this report is based on an analysis of the smart contract code itself. This report is not a prospectus or offering document, and it does not constitute an offer to sell or a solicitation of an offer to buy any securities or other financial instruments. The report should not be considered as investment, legal, tax, or other advice.

Cryptocrat makes no representation or warranty, express or implied, regarding the accuracy or completeness of the information contained in this report. Cryptocrat shall not be liable for any loss arising from the use of or reliance on this report. It is important to note that the forward-looking statements made in this report are subject to various risks and uncertainties that could cause actual results to differ materially from those expressed or implied. Cryptocrat does not undertake any obligation to update or revise any forward-looking statements, whether as a result of new information, future events, or otherwise.

Investors are advised to conduct their own thorough analysis and seek independent professional advice before making any investment decisions. The information provided in this report should be considered in the context of the specific smart contract and its associated risks.