Nexus Galaxy

Security Audit Report

16th January 2023

Security Audits
& Custom Blockchain Development

Table of Contents

Overview

Project Description

“Nexus Galaxy is an Eco-System with its Deflationary Token, Nexus Galaxy token powers NFT MarketPlaces, P2E Games with Blockchain integration, Freelancing Platform, Escrow system and much more...” By Nexus Galaxy Team

Project Information

Codebase

Codebase1:
https://github.com/adilghani/nexusgalaxy-contract
Codebase2:
https://testnet.bscscan.com/address/0x30C2F4315e2ed2c5b06a0d9cAa818a6B6f967783#code
Deployed Smart-Contract
https://bscscan.com/address/0xf5CFd25856b5fB1B2E427A52ef969012169eb772

Website: https://nexusgalaxy.io/

Twitter: https://twitter.com/nxsgalaxy

Telegram: https://t.me/nxsgalaxy

Project Details

Project Name	Nexus Galaxy
Platform	BSC
Language	Solidity
Deployed	Yes
Anon Team	No
Airdropped Tokens	No
Ico	Upcoming
Listed on dexes	Upcoming
Listed on cexes	No
Locked Liquidity	Upcoming
Team tokens vested or locked	Upcoming

Snipe Auditing Process

Steps
Manual line-by-line code reviews by multiple auditors to ensure the logic behind each function
Automated smart contract tests with priopietary scripts
Manual testing on testnet or mainnet networks
Suggest remediations or contract fixes
Provide security audit certificate

Audit Summary

Audit Delivery Date:	16th January 2023
Manual Review:	Yes
Manual test on testnet	Yes
Manual test on mainnet	No
Project Owner KYC:	Yes
Website publication:	Yes
Twitter publication:	Yes

Vulnerability Summary

Critical:	No
Medium:	Yes 1 (Fixed)
Minor:	Yes 1
Informational:	Yes 1

Vulnerabilities

Medium

LP Included on rewards distribution even if it shouldn’t be included
We suggest to include a function to exclude lp address from distribution (FIXED on codebase2)

Minor

Contract requires manual interactions to function properly

Implement swapatamount to automatically trigger the swaps and automate the rewards fees distribution when someone triggers a sell as function releaseTaxes can get stuck if amount of taxes is greater than the liquidity, in this case owner can use burn function, even if not integrated for this scope but for reducing the supply.

Informational

The owner has full access to modify some parameters of the contract such as the % of the fees, min. tokens to get the dividends and so on.
Project owner said that will change the contract’s parameters only with its community consense.

Owner Privileges

The audited smart-contract includes functions that can be called only by owner,those functions have the possibility to influence the distribution of rewards, supply, fees…

Owner Privileges:
Function releaseTaxes : this function swaps the token fees stored in the contract for BNB and then sends the BNB to backToWallet, team,marketing,development, distribution of rewards to last 5 contract's interactors.

Function createNewTokens: this function allows the contract owner to mint new tokens. This Function has been removed to protect investors after our review.

Function burnTokens: this function allows the owner to burn tokens and so reduce the total supply.

Function setNoTaxAddresses: this function allows the owner to exclude addresses from being subject to the token taxes.

Function setBackToWalletAddress: this function allows the owner to set the BackToWallet address.

Function setTeamAddress: this function allows the owner to set the TeamAddress.

Function setMarketingAddress: this function allows the owner to set the Marketing Address.

Function setDevelopmentAddress: this function allows the owner to set the Development address.

Function setOutTaxTokenAddress: this function allows the owner to set the token to receive after swapping the token itself.

Function updateRouter: this function allows the owner to set the dex to manage the contract's fees.

Function to updatefees: this function has been deleted as per our suggestion.

Tests & Relative Outputs

Transfer:

https://testnet.bscscan.com/tx/0xdefee8a11bc3de9c4f836c3e3c4454c8c0cfb041581b1a50a9dabe1ab14f8b6a

Result: Fees are taken correctly

Approve:

https://testnet.bscscan.com/tx/0xe5dc14c3be261f3591586ab94e2b692a9f588dbd077e6f53c1158d7fcb60cdd1

Result: Approved correctly

Add liquidiy:

https://testnet.bscscan.com/tx/0xf4cd14fb525ba4e0127095b26a5b733f6865a056a19bf09d1739370070891006

Result: Liquidity added Correctly

Swap BNB for Nexus:

https://testnet.bscscan.com/tx/0xf149e100a2083a3fdd27bc50b7a716f0844639494d1f5de3182016e60b393d78

Result:Swap for BNB executed correctly

Action: use BurnTokens function

https://testnet.bscscan.com/tx/0x2802c14c33109a5e8168e22ca1ab84768db0ae5b5ee5ba5af1e3249b671b09bc

Result:
Tokens Burned + Supply is updated automatically once a burn transaction is executed, this allows everyone to know the real supply on real time.

Tests & Relative Outputs

Action: use withdrawtokens function to withdraw Nexus

https://testnet.bscscan.com/tx/0x9e5e06dd13a4beac1d98304c42a805e6bded061a76fb7ec6cefe493da0a655e4

Result: Owner can withdraw tokens stored in the contract itself

Action: Mint 100 Nexus

https://testnet.bscscan.com/tx/0xf77bc2a673459cd6c2f53215f6b5769d8c733e3e78161466db7cb7ddf0ca5adf

Result: Owner minted successfully 100 tokens

Action: Buy

https://testnet.bscscan.com/tx/0xeeb13781df67eee540825da172e3f5bee8ba4e1d36695017737b2532725b95ee

Function automatically triggered: function updateAndPayRecentHolders

Result: The function included the LP contract address
Suggestion: Add exclude function to exclude the LP contract address from distribution.

Action: List on a DEX BFR approval

https://testnet.bscscan.com/tx/0xc52d295952dd6ce6303c717f1cecfd9a7ec7e653fb4a8c9113b60669293ca504

Conclusion

Coodebase 1 shouldn’t be used in production with our tests we discovered that the logic doesn’t exclude LP contract address from distribution.
This issue has been fixed on codebase 2 integrating the function to exclude the LP contract address from the distribution. However we suggest further testing.
We highly suggest to implement a logic to “automatically” trigger the following functions releaseTaxes, SwapandPayTaxes, function updateAndPayRecentHolders, a great solution could be adding the “SwapAtAmount” logic that gets triggered (and so triggers the above functions) once there is a sell after the accrued fees Amount is reached.

Codebase2 can be used in production, owner must remember to call the function releaseTaxes.

Deployed Contract: the following functions have been deleted: Minting, update fees.
The code has been reformatted and relesetaxes functions has been updated.
Deployed contract can be used safely in production.

Disclaimer

By reading this report or any part of it, you agree to the terms of this Disclaimer. This report is provided for information purposes only and on a non-reliance basis and does not constitute investment advice. No one shall have any right to rely on the report or its contents and SnipeFinance.com owns no duty of care towards you or any other person, nor does Snipefinance.com make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided as is, without any conditions, warranties or other terms of any kind except as set out in this disclaimer, SnipeFinance.com hereby excludes all representations, warranties, conditions and other terms, SnipeFinance.com hereby excludes all liability and responsibility and neither you nor any other person shall have any claim against SnipeFinance.com for any amount or kind of loss or damage that may result to you or any other person(including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and water in delict, tort(including without limitations negligence), contract, breach of statutory duty, misinterpretation (weather innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intended 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. SnipeFinance.com positions that each company and individual are responsible for their own due diligence and continuous security.
SnipeFinance.com 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 analysis of the security is purely based on the smart contracts alone.
No applications or operations were reviewed for security. No product code has been reviewed.

Snipefinance.com is a blockchain development agency run by italian developers that works with startups, SMBs & enterprises.
We help companies build their own digital products from scratch into a real and sustainable blockchain business.
Our main services include custom blockchain development & Security Audits, our auditing proccess consist in analyzing many aspects of the project to provide a complete and easy to understand report for the involved community.