KRONICLABZ AUDITS

Security Assessment

Pluto Alliance Staking

April 13, 2022

Table of Contents

Audit Summary

This report has been prepared for Pluto Alliance Staking on the Ethereum Mainnet network. KronicLabs and CFGNINJA provides both client-centered and user-centered examination of the smart contracts and their current status when applicable. This report represents the security assessment made to find issues and vulnerabilities on the source code along with the current liquidity and token holder statistics of the protocol.

A comprehensive examination has been performed, utilizing Cross Referencing, Static Analysis, In-House Security Tools, and line-by-line Manual Review.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Inspecting liquidity and holders statistics to inform the current status to both users and client when applicable.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Verifying contract functions that allow trusted and/or untrusted actors to mint, lock, pause, and transfer assets.

Project Overview

Token Summary

Parameter	Result
Address	0x882eA36F2031F3EDD6Cc243472f6Bea7195ECaf3
Name	Pluto Alliance
Token Tracker	Pluto Alliance (N/A)
Decimals	0
Supply	0
Platform	Ethereum Mainnet
compiler	v0.8.13+commit.abaa5c0e
Contract Name	StakeNFT
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://etherscan.io/address/0x882eA36F2031F3EDD6Cc243472f6Bea7195ECaf3
Url	https://plutoalliance.com

Main Contract Assessed Contract Name

Name	Contract	Live
Pluto Alliance	0x882eA36F2031F3EDD6Cc243472f6Bea7195ECaf3	Yes

TestNet Contract Assessed Contract Name

Name	Contract	Live
Pluto Alliance	0xa06cd880725cdbf6989d60949cc7c2998cc55481	Yes

Solidity Code Provided

SolID	FileNameMD5	FileName
plutoalliance	cbe834eb63d2381bf4689043cea61ac67887bffa	plutoalliance.sol

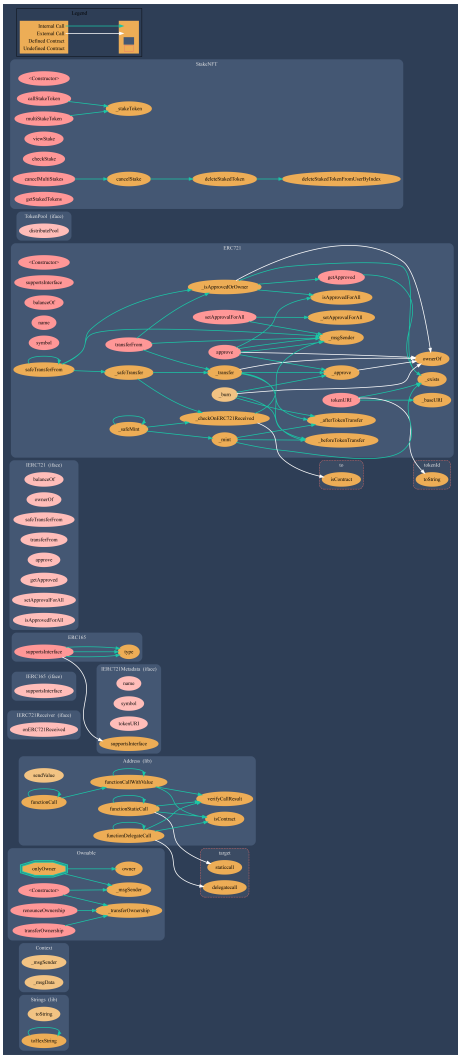
Smart Contract Vulnerability Checks

Vulnerability	Automatic Scan	Manual Scan	Result
Unencrypted Private Data On-Chain	Complete	Complete	Low / No Risk
Code With No Effects	Complete	Complete	Low / No Risk
Message call with hardcoded gas amount	Complete	Complete	Low / No Risk
Hash Collisions With Multiple Variable Length Arguments	Complete	Complete	Low / No Risk
Unexpected Ether balance	Complete	Complete	Low / No Risk
Presence of unused variables	Complete	Complete	Low / No Risk
Right-To-Left-Override control character (U+202E)	Complete	Complete	Low / No Risk
Typographical Error	Complete	Complete	Low / No Risk
DoS With Block Gas Limit	Complete	Complete	Low / No Risk
Insufficient Gas Griefing	Complete	Complete	Low / No Risk
Incorrect Inheritance Order	Complete	Complete	Low / No Risk
Write to Arbitrary Storage Location	Complete	Complete	Low / No Risk
Requirement Violation	Complete	Complete	Low / No Risk
Missing Protection against Signature Replay Attacks	Complete	Complete	Low / No Risk
Weak Sources of Randomness from Chain Attributes	Complete	Complete	Low / No Risk

Call Graph and Inheritance

The contract for Pluto Alliance has the following call graph structure

The Project has a Total Supply of 0 and has the following inheritance



Contract Ownership

The contract ownership of Pluto Alliance is not currently renounced. The ownership of the contract grants special powers to the protocol creators, making them the sole addresses that can call sensible ownable functions that may alter the state of the protocol.

The current owner is the address 0xB9A59DCa6ACfEad64391061Ff762957f579bba21 which can be viewed from:
HERE

The owner wallet has the power to call the functions displayed on the priviliged functions chart below, if the owner wallet is compromised this privileges could be exploited.

We recommend the team to renounce ownership at the right timing if possible, or gradually migrate to a timelock with governing functionalities in respect of transparency and safety considerations.

We recommend the team to use a Multisignature Wallet if contract is not going to be renounced, this will give the ability to the team to have more control over the contract.

KYC Information

The Project Onwers of Pluto Alliance has provided KYC Documentation.

KYC Certificated can be found on the Following:
KYC Data

KYC Information Notes:

Auditor Notes: Auditor asked project owner if there was any plans to KYC.

Project Owner Notes: No response during this time from the Main Auditor, this can be updated at a later time.

Mythx Security Summary Checks

ID	Severity	Name	File	location
SWC-103	Low	A floating pragma is set.	plutoalliance.sol	L: 9 C: 0
SWC-103	Low	A floating pragma is set.	plutoalliance.sol	L: 79 C: 0
SWC-103	Low	A floating pragma is set.	plutoalliance.sol	L: 106 C: 0
SWC-103	Low	A floating pragma is set.	plutoalliance.sol	L: 184 C: 0
SWC-103	Low	A floating pragma is set.	plutoalliance.sol	L: 409 C: 0
SWC-103	Low	A floating pragma is set.	plutoalliance.sol	L: 439 C: 0
SWC-103	Low	A floating pragma is set.	plutoalliance.sol	L: 467 C: 0
SWC-103	Low	A floating pragma is set.	plutoalliance.sol	L: 498 C: 0
SWC-103	Low	A floating pragma is set.	plutoalliance.sol	L: 643 C: 0
SWC-103	Low	A floating pragma is set.	plutoalliance.sol	L: 672 C: 0
SWC-107	Low	Read of persistent state following external call.	plutoalliance.sol	L: 1120 C: 0
SWC-107	Low	Read of persistent state following external call.	plutoalliance.sol	L: 1187 C: 8

ID	Severity	Name	File	location
SWC-107	Low	Read of persistent state following external call.	plutoalliance.sol	L: 1190 C: 8
SWC-107	Low	Read of persistent state following external call.	plutoalliance.sol	L: 1191 C: 8
SWC-107	Low	Write to persistent state following external call.	plutoalliance.sol	L: 1180 C: 8
SWC-108	Low	State variable visibility is not set..	plutoalliance.sol	L: 1131 C: 14
SWC-108	Low	State variable visibility is not set.	plutoalliance.sol	L: 1132 C: 12
SWC-108	Low	State variable visibility is not set.	plutoalliance.sol	L: 1157 C: 33
SWC-113	Low	Multiple calls are executed in the same transaction.	plutoalliance.sol	L: 1180 C: 8
SWC-116	Low	A control flow decision is made based on The block.timestamp environment variable.	plutoalliance.sol	L: 1205 C: 8

We scan the contract for additional security issues using MYTHX and industry standard security scanning tool

Priviliged Functions

Function Name	Parameters	Visibility
checkStake	tokenid	public

Important Notes To The Users:

- Kroniclabz and CFG Ninja Deployed the staking contract to testnet, during our code review we identified some key areas of improvement or review.
- Customer should review the current code inheritance and validate if that was intended for the code, there are a few areas of improvement.
- No high-risk Exploits/Vulnerabilities Were Found in the Source Code.
- Security scan did not identified mayor issues with code.
- This audit has been performed by the CFG Ninja Team and Kroniclabz Team in a join venture.
- Customer social media present is very good one, all other areas of the audit and team looks great.

Audit Passed

Social Media Checks

Social Media	URL	Result
Twitter	https://twitter.com/Pluto_Alliance	Pass
Instagram	https://instagram.com/pluto.alliance/	Pass
Website	https://plutoalliance.com	Pass
Telegram	https://t.me/the_pluto_alliance	Pass

We recommend to have 3 or more social media sources including a completed working websites.

Social Media Information Notes:

Auditor Notes: undefined

Project Owner Notes: http://discord.gg/plutoalliance

Disclaimer

KronicLabs and CFGNINJA has conducted an independent audit to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the codes that were provided for the scope of this audit. This audit report does not constitute agreement, acceptance or advocation for the Project that was audited, and users relying on this audit report should not consider this as having any merit for financial advice in any shape, form or nature. The contracts audited do not account for any economic developments that may be pursued by the Project in question, and that the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are completely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence regardless of the findings presented in this report. Information is provided 'as is', and KronicLabs and CFGNINJA is under no covenant to the completeness, accuracy or solidity of the contracts audited. In no event will KronicLabs and CFGNINJA or its partners, employees, agents or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions and/or actions with regards to the information provided in this audit report.

The assessment services provided by KronicLabs and CFGNINJA is subject to dependencies and 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.