PEX AUDIT

PEX Audit

SMART CONTRACT

Security Audit Report

PEX Audit

Project
UXOS NFT

UXOS

The Future Is Now.

Audit Details

Project: UXOS NFT

Blockchain: BSC

Project website:
uxos-ai.com

Authors: PEX Audit team DM

Date: April 30th, 2023

Disclaimer

PEX audits and reports should not be considered as a form of project's "advertisement" and does not cover any interaction and assessment from "project's contract" to "external contracts" such as Pancakeswap or similar.

PEX does not provide any warranty on its released reports.

PEX should not be used as a decision to invest into an audited project please do your own research. PEX provides transparent reports to all its "clients" and to its "clients participants" and will not claim any guarantee of bug-free code within its SMART CONTRACT.

PEX presence is to analyze, audit and assess the client's smart contract's code.

Each company or project shall be liable for its own security flaws and functionalities.

Scope of Work & Background

The main scope of this report/audit, is to document an accurate assessment of the condition of the smart contract and whether it has any security flaws in the implementation of the contract.

UXOS team agreed and provided us with the files that needed to be tested (Through Github, Etherscan, files, etc.). PEX will be focusing on contract issues and functionalities along with the projects claims from smart contract to their website, whitepaper and repository where available, which has been provided by the project.

Code is reviewed manually and with the use of software using industry best practices.

Background

PEX was contracted by **UXOS** team to perform the security audit of the smart contract code:

- Contract Address 0x3077E6c3D96ffbbc1DD13809aCcbB9665247ceA4

The purpose of the audit was to achieve the following:

- Ensure that the claimed functions exist and function correctly.
- Identify any security vulnerabilities that may be present in the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Project Description from Dev's

UXOS NFT minting

Social Media Links

Telegram: uxostoken

Twitter: UXOS AI

Medium: N/A

Facebook: N/A

Discord: N/A

Contracts details

Contract details for April 30th, 2023

Contract/Project name: UXOS NFT

Description: NFT minting contract

Compiler version: v0.8.17

Contract address: 0x3077E6c3D96ffbbc1DD13809aCcbB9665247ceA4

Contract deployer address: 0x0A082068Fa05253eAB2EaeD698edA443C57452c2

Contract's current owner address: 0x923dde2109810fbe4ff08aa14fa09de2ccfabcbb

Dev's KYC: Yes Fuddoxx

Contract write functions details

Owner privileges:

Contract contains owner control, which does not make it fully decentralised , the owner has privileges, and has authority to make any changes now.

Centralization

This smart contract has some functions which can be executed by the Admin (Owner) only.

1. approve
2. mint
3. pause
4. renounceOwnership
5. reveal
6. safeTransferFrom
7. safeTransferFrom
8. setApprovalForAll
9. setBaseExtension
10. setBaseURI
11. setCost
12. setNotReavealedURI
13. setmaxMintAmount
14. transferFrom
15. transferOwnership
16. withdraw

To make the smart contract 100% decentralized, we suggest renouncing ownership in the smart contract once its function is completed.

SWC Registry: Smart Contract Weakness/Vulnerabilities

SWC-136	Unencrypted Private Data On-Chain	PASSED
SWC-135	Code With No Effects	PASSED
SWC-134	Message call with hardcoded gas amount	PASSED
SWC-133	Hash Collisions with Multiple Variable Length Arguments	PASSED
SWC-132	Unexpected Ether balance	PASSED
SWC-131	Presence of unused variables	PASSED
SWC-130	Right-To-Left-Override control character (U+202E)	PASSED
SWC-129	Typographical Error	PASSED

SWC-128	DoS With Block Gas Limit	PASSED
SWC-127	Arbitrary Jump with Function Type Variable	PASSED
SWC-126	Insufficient Gas Griefing	PASSED
SWC-125	Incorrect Inheritance Order	PASSED
SWC-124	Write to Arbitrary Storage Location	PASSED
SWC-123	Requirement Violation	LOW ISSUE
SWC-122	Lack of Proper Signature Verification	PASSED
SWC-119	Shadowing State Variables	PASSED

SWC-118	Incorrect Constructor Name	PASSED
SWC-120	Weak Sources of Randomness from Chain Attributes	PASSED
SWC-117	Signature Malleability	PASSED
SWC-116	Block values as a proxy for time	PASSED
SWC-115	Authorization through tx.origin	PASSED
SWC-114	Transaction Order Dependence	PASSED
SWC-121	Missing Protection against Signature Replay Attacks	PASSED
SWC-113	DoS with Failed Call	PASSED

SWC-112	Delegatecall to Untrusted Callee	PASSED
SWC-111	Use of Deprecated Solidity Functions	PASSED
SWC-110	Assert Violation	PASSED
SWC-109	Uninitialized Storage Pointer	PASSED
SWC-108	State Variable Default Visibility	LOW ISSUE
SWC-107	Reentrancy	PASSED
SWC-106	Unprotected SELFDESTRUCT Instruction	PASSED
SWC-105	Unprotected Ether Withdrawal	PASSED

SWC-104	Unchecked Call Return Value	PASSED
SWC-103	Floating Pragma	LOW ISSUE
SWC-102	Outdated Compiler Version	PASSED
SWC-101	Integer Overflow and Underflow	PASSED

Low issue = Low-level weakness/vulnerabilities are mostly related to outdated, unused etc. code snippets, that can't have significant impact on execution
Medium severity = Medium-level vulnerabilities are more important; however, they can't lead to tokens lose
High severity = critical, immediate danger of exploitation
SOLHINT LINTER, Solidity Static Analysis using REMIX IDE did not find any serious issues.
Contract Deployed and tested on Remix VM.

Issue Checking

Manual code review is satisfactory.

CLOSING NOTES

Investors Advice: Technical audit of the smart contract does not guarantee the ethical nature of the project. Any owner controlled functions should be executed by the owner with responsibility. All investors/users are advised to do their due diligence before investing in the project.

Always make sure to always inspect all values and variables.
This includes, but is not limited to: • Ownership • Proper Ownership Renouncement (if any) • Any other owner-adjustable settings or variables.

OVERALL ASSESSMENT

SATISFACTORY