Security Assessment

WazirX

May 21st, 2021

Table of Contents

Summary

This report has been prepared for WazirX smart contracts, to discover issues and vulnerabilities in the source code of their Smart Contract as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis and Manual Review techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Enhance general coding practices for better structures of source codes;
- Add enough unit tests to cover the possible use cases given they are currently missing in the repository;
- Provide more comments per each function for readability, especially contracts are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

Overview

Project Summary

Project Name	WazirX
Description	WazirXNFT + Sale
Platform	BSC
Language	Solidity
Codebase	https://github.com/WazirXNFT/NFTMarketplace/tree/audit
Commit	<858f11a539bb47decabacc11b5ee4af452c143fb>

Audit Summary

Delivery Date	May 21, 2021
Audit Methodology	Static Analysis, Manual Review
Key Components	

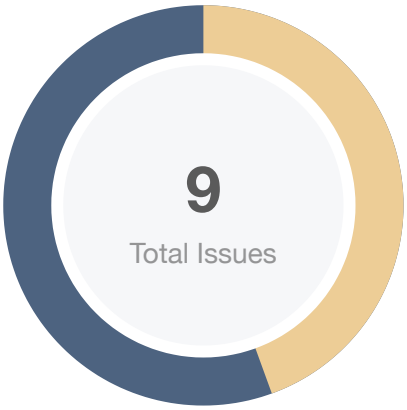
Vulnerability Summary

Total Issues	9
Critical	0
Major	0
Medium	0
Minor	4
Informational	5
Discussion	0

Audit Scope

ID	file	SHA256 Checksum
ERC	ERC721Full.sol	d8c42a567f731b8a6d132be8098ed6e0b1cc360467420358c438e37da38f1ef1
EWX	Escrow.sol	df16e8e34257c115d0cce493ef29a604960bddb1006b965fba5be21756231e64
IEW	IEscrow.sol	1181b3cb0a67fc4c1c1945daf4cc4ff2a022b2e5aad0a5c4bf50687ca677a06d
IWX	IWazirXNFT.sol	9417d16aaf700fa360821ffdafe063188414d80627bbca46f7fab3fdcafe84b5
MWX	Migrations.sol	36843b9bddd31153133949f23ce65cd0fa2d91cc5f0ac36298ba07d39de7fecd
WXN	WazirXNFT.sol	5fb204350d8eeaa67e050968905f357e95f93c2ff9fedd1ee5749020428a7a7d
WXW	sale.sol	da5763f1d4ab204a939fee6c53cced091eda0d4639e1ad09116f40e66e964906

Findings



Critical	**0** (0.00%)
Major	**0** (0.00%)
Medium	**0** (0.00%)
Minor	**4** (44.44%)
Informational	**5** (55.56%)
Discussion	**0** (0.00%)

ID	Title	Category	Severity	Status
EWX-01	Privileged Ownerships on Escrow	**Centralization / Privilege**	**Minor**	**Partially Resolved**
EWX-02	Missing Zero Address Validation	Volatile Code	Minor	Resolved
EWX-03	Missing Emit Events	Gas Optimization	Informational	Resolved
EWX-04	Proper Usage of public and external	Gas Optimization	Informational	Resolved
WXN-01	Missing Zero Address Validation	Volatile Code	Minor	Resolved
WXN-02	Deprecated Function	Compiler Error	Informational	Resolved
WXW-01	Missing Emit Events	Gas Optimization	Informational	Resolved
WXW-02	Privileged Ownerships on Sale	**Centralization / Privilege**	**Minor**	**Acknowledged**
WXW-03	Redundant Check of BEP20.balanceOf	Volatile Code	Informational	Resolved

EWX-01 | Privileged Ownerships on Escrow

Category	Severity	Location	Status
Centralization / Privilege	**Minor**	Escrow.sol: 41	**Partially Resolved**

Description

The owner of `Escrow` can set contract approval, who is able to transfer tokens locked in the `Escrow` to an external address.

Recommendation

We advise the client to adopt:

1. Time lock feature with reason and delay to set contract approval.
2. Multi-signature requirement with community-selected 3rd-party independent co-signers, and/or DAO with transparent governance within the project's community to manage sensitive role accesses.

These would allow the community monitor in respect of transparency considerations.

Alleviation

[WazirX Team]: The contract owner will be a multisig wallet. We will be deploying contracts using a non-multisig wallet & then transferring the ownership to a multisig wallet

EWX-02 | Missing Zero Address Validation

Category	Severity	Location	Status
Volatile Code	Minor	Escrow.sol: 28	Resolved

Description

Missing validation for the input variables `_to` in function `createToken` and `transferToken`.

Recommendation

Check that the address is not zero by adding following checks.

```
require(_to != address(0),"createToken: zero address!");
```

Alleviation

The update has been applied to WazirXNFT and Escrow contract.

EWX-03 | Missing Emit Events

Category	Severity	Location	Status
Gas Optimization	Informational	Escrow.sol: 41	Resolved

Description

The function that affects the status of sensitive variables should be able to emit events as notifications to customers. in Sale.sol: `setServiceAccount` `setServiceComission()` `setCreatorRoyaltyLimit`

in Escrow.sol: `setContractApproval()`

Recommendation

Recommend emitting events, for all the essential state variables that are possible to be changed during runtime.

Alleviation

The update has been applied to sale contract.

EWX-04 | Proper Usage of public and external

Category	Severity	Location	Status
Gas Optimization	Informational	Escrow.sol: 53	Resolved

Description

Functions which are never called internally within the contract should have external visibility.
`isContractApproved`

Recommendation

We recommend changing the visibility of the aforementioned function to external.

Alleviation

The update has been applied to Escrow contract.

WXN-01 | Missing Zero Address Validation

Category	Severity	Location	Status
Volatile Code	Minor	WazirXNFT.sol: 31	Resolved

Description

Missing validation for the input variables `_to` in function `createToken` and `transferToken`.

Recommendation

Check that the address is not zero by adding following checks.

```
require(_to != address(0),"createToken: zero address!");
```

Alleviation

The update has been applied to WazirXNFT and Escrow contract.

WXN-02 | Deprecated Function

Category	Severity	Location	Status
Compiler Error	Informational	WazirXNFT.sol: 43	Resolved

Description

Since Openzeppelin library version of 4.1.0, function `_setTokenURI(_tokenId, _tokenURI)` has been removed.

Recommendation

You can override `tokenURI` with your required logic in ERC721Full.

Sample code:

```
function _setTokenURI(uint256 tokenId, string memory _tokenURI) internal virtual {
            require(_exists(tokenId), "ERC721Metadata: URI set of nonexistent token");
            _tokenURIs[tokenId] = _tokenURI;
        }
```

Alleviation

The update has been applied to ERC721Full.
https://github.com/WazirXNFT/NFTMarketplace/commit/55059e616ab221189c7b05a657161687793447fb
.

WXW-01 | Missing Emit Events

Category	Severity	Location	Status
Gas Optimization	Informational	sale.sol: 130, 139, 147	Resolved

Description

The function that affects the status of sensitive variables should be able to emit events as notifications to customers. in Sale.sol: `setServiceAccount` `setServiceComission()` `setCreatorRoyaltyLimit`

in Escrow.sol: `setContractApproval()`

Recommendation

Recommend emitting events, for all the essential state variables that are possible to be changed during runtime.

Alleviation

The update has been applied to sale contract.

WXW-02 | Privileged Ownerships on Sale

Category	Severity	Location	Status
Centralization / Privilege	**Minor**	sale.sol	**Acknowledged**

Description

The owner of contract `sale` has the permission to:

1. Set service comission
2. Set service account
3. Set Creator Royalty Limit

without obtaining the consensus of the community.

Recommendation

Renounce ownership when it is the right timing, or gradually migrate to a timelock plus multisig governing procedure and let the community monitor in respect of transparency considerations.

Alleviation

The team acknowledged this finding.

WXW-03 | Redundant Check of BEP20.balanceOf

Category	Severity	Location	Status
Volatile Code	Informational	sale.sol: 257~258	Resolved

Description

Check of BEP20.balanceOf in L257 is redundant since the check has been performed in L190.

Recommendation

Remove the balance check in L257.

Alleviation

The update has been applied to sale contract.

Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.

Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimal EVM opcodes resulting in a reduction on the total gas cost of a transaction.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that may result in a vulnerability.

Compiler Error

Compiler Error findings refer to an error in the structure of the code that renders it impossible to compile using the specified version of the project.

Checksum Calculation Method

The "Checksum" field in the "Audit Scope" section is calculated as the SHA-256 (Secure Hash Algorithm 2 with digest size of 256 bits) digest of the content of each file hosted in the listed source repository under the specified commit.

The result is hexadecimal encoded and is the same as the output of the Linux "sha256sum" command against the target file.

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to the Company in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes without CertiK'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 considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts CertiK to perform a security assessment. This report 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 in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing 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. CertiK's position is that each company and individual are responsible for their own due diligence and continuous security. CertiK'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.

About

Founded in 2017 by leading academics in the field of Computer Science from both Yale and Columbia University, CertiK is a leading blockchain security company that serves to verify the security and correctness of smart contracts and blockchain-based protocols. Through the utilization of our world-class technical expertise, alongside our proprietary, innovative tech, we're able to support the success of our clients with best-in-class security, all whilst realizing our overarching vision; provable trust for all throughout all facets of blockchain.