Guild Audits

SEPTEMBER 2022

THE WICRYPT OUTLINER SMART CONTRACT AUDIT REPORT

By Guild Audits

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Description:

The Wicrypt NFT is a smart contract that allows for the mint of ERC721 token that serves as a digital representation of the Wicrypt device. The contract inherits ERC721Enumerable, ReentrancyGuard, and Ownable; these contracts respectively aids in the enumeration of tokens, guard against possible reentrancy attacks, and provide ownership management.

PROJECT AUDIT SCOPE AND FINDINGS

The motive of this audit is to review the codebase of Wicrypt contracts for the purpose of achieving secured, corrected and quality contracts.

Number of Contracts in Scope:

- **WicryptDevice**

Link to Project codebase:
https://polygonscan.com/address/0x0d2dd4f745A6FE105932825FA084b7Aa6B582A10#code

Duration for Audit: September 07, 2022 to September 11, 2021

Audit Methodology:

Issues found:

MODE OF AUDIT AND METHODOLOGIES

The mode of audit carried out in this audit process is as follow:

- **Manual Review**: This is the first and principal step carried out to understand the business logic behind a project. At this point, it involves research, discussion and establishment of familiarity with contracts. Manual review is critical to understand the nitty-gritty of the contracts.
- **Automated Testing:** This is the running of tests with audit tools to further cement discoveries from the manual review. After a manual review of a contract, the audit tools which could be Slither, Echidna, or Mythril are run on the contract to find out issues.
- **Functional Testing:** Functional testing involves manually running unit, static, and dynamic testing. This is done to find out possible exploit scenarios that could be used to steal money from the contracts. This helps understand the functionality of the contracts and find out lapses in the reverts check in contract.

The methodologies for establishing severity issues:

- High Level Severity Issues
- Medium Level Severity Issues
- Low Level Severity Issues
- Informational Level Severity Issues

REPORT OF FINDINGS

HIGH SEVERITY ISSUES

- **No Issues Found.**

MEDIUM SEVERITY ISSUES

- **No Issues Found**

LOW SEVERITY ISSUES

- **Missing Events for Critical Operations**
  - Whenever a function which is sensitive and is controlled by a centralized role, it is recommended to always emit an event

Recommendation:
Consider emitting an event to functions, that are controlled by Admin(onlyOwner)

Status: Resolved

- **Missing zero check**
  - Contracts lack zero address checks, hence are prone to be initialized with zero addresses.

Recommendation:
Consider adding zero address checks in order to avoid risks of incorrect contract initializations.

Status: Resolved

- **Transfer Depreciated**
  - To Transferring Ether from one account to another the use of account.send and account.transfer has been deprecated, because .send use all 2300 gas and return bool , transfer use 2300 gas and revert, while .call forward all gas or you set the gas and return bool
  -

Recommendation:
Consider using .call because it allow you to set the gas and return a bool

Status: Resolved

INFORMATIONAL SEVERITY ISSUES

- **No Issues Found.**

CLOSING SUMMARY

There were discoveries of some low issues after the audit. The audit team thereafter suggested some remediation to help remedy the issues found in the contract.

APPENDIX

- *Audit: The review and testing of contracts to find bugs.*
- *Issues: These are possible bugs that could lead exploits or help redefine the contracts better.*
- *Slither: A tool used to automatically find bugs in a contract.*
- *Severity: This explains the status of a bug.*

DISCLAIMER

While the audit report is aimed at achieving a quality codebase with assured security and correctness, it should not be interpreted as a guide or or recommendation for people to invest in **Wicrypt** contracts.

With smart contract audit being a multifaceted process, we admonish the **Wicrypt** team to carry out further audit from other audit firms or provide a bug bounty program to ensure that more critical audit is done to the contract.

GUILD AUDITS

Guild Audits is geared towards providing blockchain and smart contract security in the fuming web3 world. The firm is passionate about remedying the constant hacks and exploits that deters the web3 motive.