ITISH

AUDIT COMPANY

Audit Details

Audited project

0x3B07D3A964B6bEA4415C09bbE49d04DEa6105819

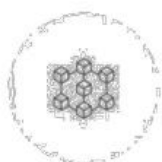**Deployer address**

0xF7A999c5255bA8197425A0756a195a47352C5998

Client contacts:

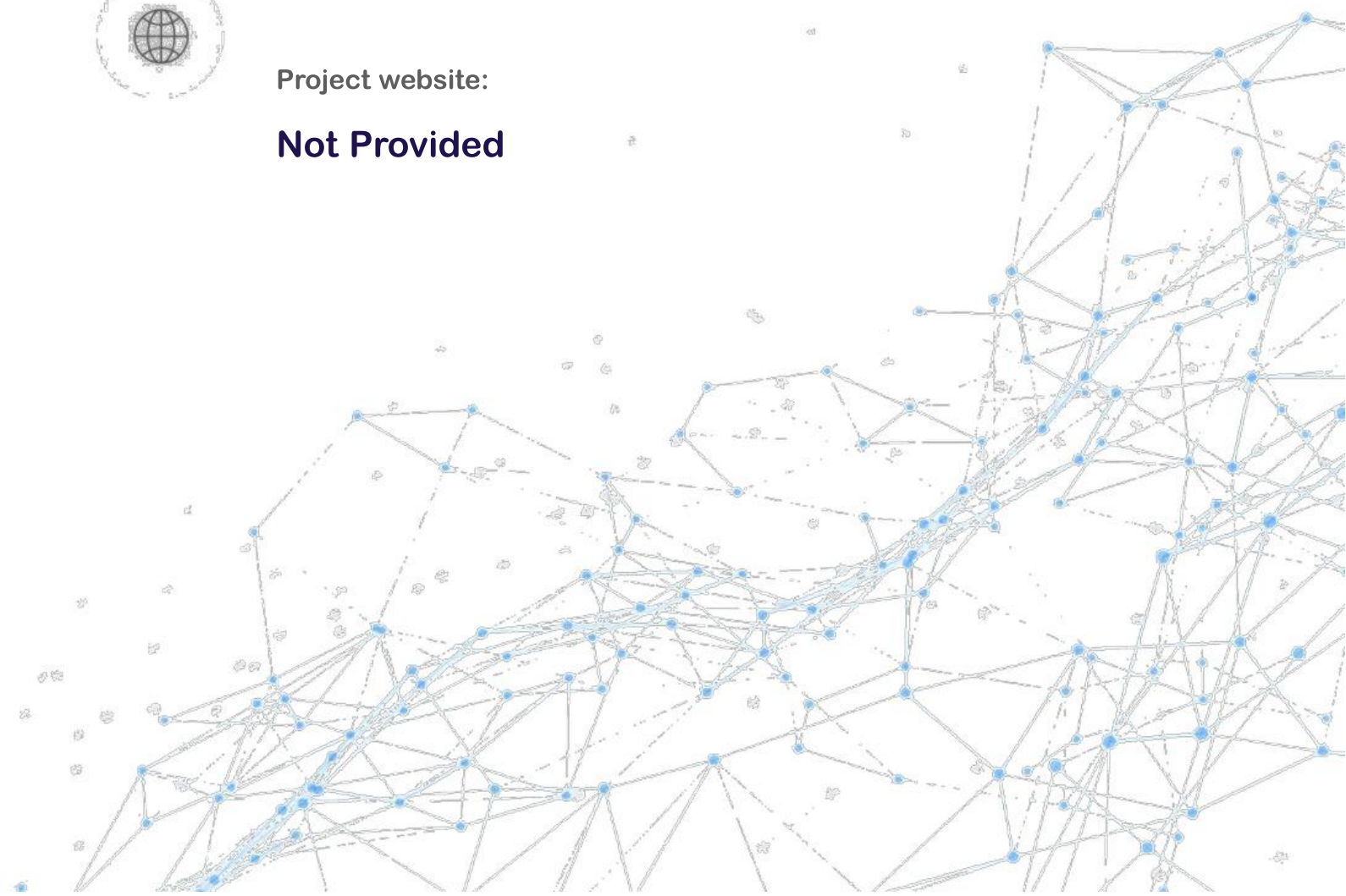https://discord.com/invite/degenheroesnft

Blockchain

Ethereum

Project website:

Not Provided

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. 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 Itish and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (Itish) owe no duty of care towards you or any other person, nor does Itish 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, and Itish hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, Itish hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Itish, 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 whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether 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.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.

Background

Itish was commissioned by 'Degen Heroes' to perform an audit of smart contracts:

https://rinkeby.etherscan.io/address/0x3b07d3a964b6bea4415c09bbe49d04dea6105819#code

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.

- Identify potential security issues with 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.

Contracts Details

Token Contract Details For 20.02.2022

Contract name
NFT

Contract address
0x3B07D3A964B6bEA4415C09bbE49d04DEa6105819

Token Creator
0xF7A999c5255bA8197425A0756a195a47352C5998

Risk Level
Low

Issues Checking Status

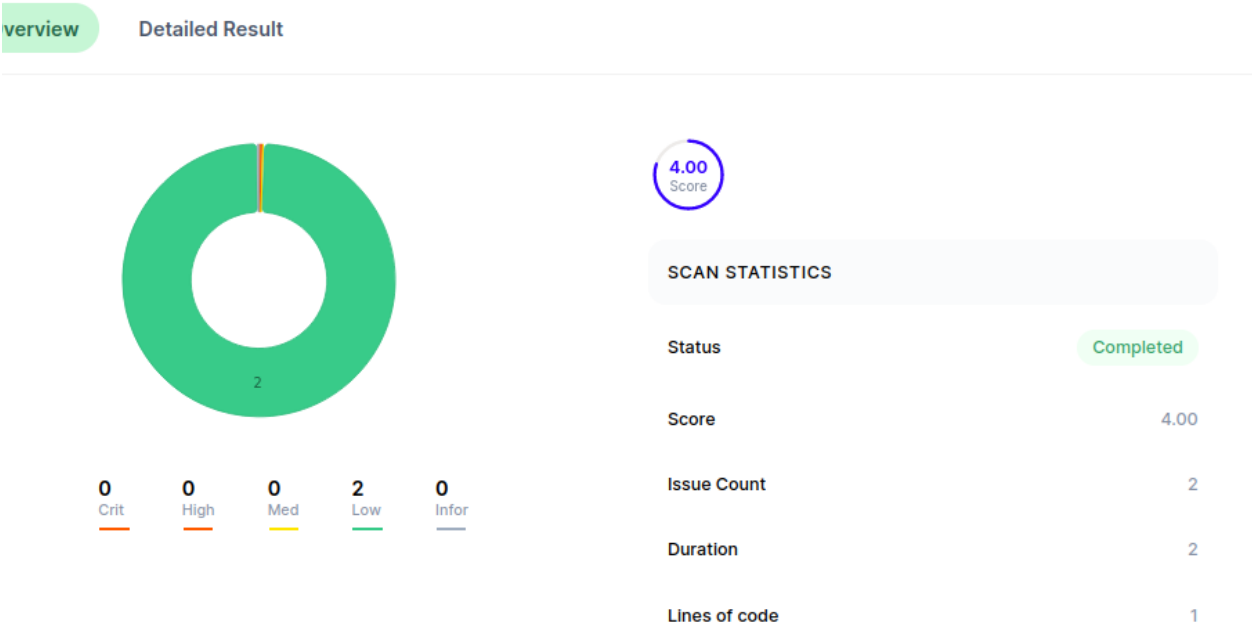| Issue description	Checking status
1. Compiler errors.	Passed
2. Compiler Compatibilities	Moderate
3. Possible delays in data delivery.	Passed
4. Oracle calls.	Passed
5. Front running.	Passed
6. Timestamp dependence.	Passed
7. Integer Overflow and Underflow.	Passed
8. DoS with Revert.	Passed
9. DoS with block gas limit.	Passed
10 Methods execution permissions.	Passed
11. Economy model of the contract.	Passed
12 The Impact of The Exchange Rate On The Logic.	Moderate
13. Private user data leaks.	Passed
14 Malicious Event log.	Passed
15. Scoping and Declarations.	Passed
16 Uninitialized storage pointers.	Passed
17. Arithmetic accuracy.	Passed
18 Design Logic.	Good

19.	Cross-function race conditions.	Passed
20.	Safe Open Zeppelin contracts implementation and usage.	Passed
21.	Fallback function security.	Passed

Security Issues

verview   Detailed Result

4.00 Score

SCAN STATISTICS	
Status	Completed
Score	4.00
Issue Count	2
Duration	2
Lines of code	1

0	0	0	2	0
Crit	High	Med	Low	Infor

✓ High Severity Issues

No Severity Issues Found.

✓ Medium Severity Issues

No Medium Severity Issues Found.

Low Severity Issues

Two Low Severity Issues Found.

0 Crit	**0** High	**0** Med	**2** Low	**0** Infor

● OUTDATED COMPILER VERSION   1 file ▼

    contract.sol

● COMPILER VERSION TOO RECENT   1 file ▶

contract.sol

```
1      // File: @openzeppelin/contracts/utils/Counters.sol
2
3
4      // OpenZeppelin Contracts v4.4.1 (utils/Counters.sol)
5
6      pragma solidity ^0.8.0;
7
8      /**
9       * @title Counters
10      * @author Matt Condon (@shrugs)
```

Vulnerability Description   Remediation

OUTDATED COMPILER VERSION

Using an outdated compiler version can be problematic especially if there are publicly disclosed bugs and issues that affect the current compiler version.

It should also be noted that the Solidity version 0.5.0 introduced some breaking changes.

Overview   **Detailed Result**

0 Crit	**0** High	**0** Med	**2** Low	**0** Infor

● OUTDATED COMPILER VERSION   1 file ▶

● COMPILER VERSION TOO RECENT   1 file ▼

    contract.sol

contract.sol

```
1      // File: @openzeppelin/contracts/utils/Counters.sol
2
3
4      // OpenZeppelin Contracts v4.4.1 (utils/Counters.sol)
5
6      pragma solidity ^0.8.0;
7
8      /**
9       * @title Counters
10      * @author Matt Condon (@shrugs)
```

Vulnerability Description   Remediation

COMPILER VERSION TOO RECENT

The compiler version detected in the code is too recent. Therefore it is not time-tested and may be susceptible to multiple bugs and vulnerabilities, both from the usage and security perspectives.

REMEDIATION METHOD ISSUE NO 1:

It is recommended to use a recent version of the Solidity compiler, preferably something above 0.8.4+ that patches most of the vulnerabilities introduced in older compiler versions.

REMEDIATION METHOD ISSUE NO 2:

It is suggested to use a compiler version that is neither too recent nor too old. A stable compiler version should be used that is time-tested by the community, which fixes vulnerabilities introduced in older compiler versions.

The code should be kept updated according to the compiler release cycle. It should be tested before going on the mainnet to reduce the chances of new vulnerabilities being introduced.

Conclusion

Smart contracts contain High severity issues! Liquidity pair contract's security is not checked due to out of scope.

LIQUIDITY LOCKING DETAILS NOT PROVIDED BY THE TEAM.

Itish note:

Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.