# **RISK AUDIT**

for



on

April 13, 2025





## **Executive Summary**

#### Report



TOTAL
Low risk
April 13, 2025

#### **Abstract**

Fidesium's automated risk assessment service was requested to perform a risk posture audit on Novel Labss contracts

#### Repository Link:

https://github.com/mutantcartel/mutant-hound-contracts.git

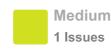
Initial Commit Hash:

8860b38f1dab16fcdd5472e1df2ebe7b0ff2a1e1

#### **Issue Summary**











#### **Caveats**

This audit was conducted at commit 8860b38f1dab16fcdd5472e1df2ebe7b0ff2a1e1. Access to the deployed contracts was not provided, and onchain data was not analyzed.

## **Test Approach**

Fidesium performed both Whitebox and Blackbox testing, as per the scope of the engagement, and relied on automated security testing.

#### Methodology

The assessment methodology covered a range of phases and employed various tools, including but not limited to the following:

- Mapping Content and Functionality of API
- Application Logic Flaws
- Access Handling
- Authentication/Authorization Flaws
- Brute Force Attempt
- Input Handling
- Source Code Review
- Fuzzing of all input parameter
- Dependency Analysis

#### **Severity Definitions**

Critical	The issue can cause large economic losses, large-scale data disorder or loss of control of authority management.	
High	The issue puts users' sensitive information at risk or is likely to lead to catastrophic financial implications.	
Medium	The issue puts a subset of users' sensitive information at risk, reputation damage or moderate financial impact.	
Low	The risk is relatively small and could not be exploited on a recurring basis, or is low-impact to the client's business.	
Informational	The issue does not pose an immediate risk but is relevant to security best practices or defence in Depth.	



# Risk Issues

Vunerability	Description	Risk	Probability	Status
Interface noncompliance: ERC5192 with transfer	Contract claims to support ERC5192 interface while allowing transfer	High	High	Active
Missing existence check	locked is missing an exitence check on tokenId	Medium	Medium	Active
Unnecessary Storage Gap	The contract is not upgradeable, but implements a storage gap	Info	Info	Active
Missing event	mintfunction does not emit events.	Info	Info	Active



## **Risk Overview**

#### **Team Risk**

Low risk: 1

No issues found in founding team

Doxxing Status	Team Experience	Risk Summary
Public	Highly relevant	Low

## Liquidity

Risk summary: N/A

As this is a Github assessment, liquidity risks have not been assessed

#### **Whale Concentration**

Risk summary: N/A

As this is a Github assessment, whale risks have not been assessed

#### **Smart Contract Risks**

Risk summary: 19

The contract is mostly well written, but has a handful of significant flaws that need to be carefuly managed, and expose the ecosystem to a variety of risks, including price manipulation attacks and loss of funds.



## **Vulnerabilities Critical**

#### **Current scan criticals Clear**

During this scan no critical security vulnerabilities were identified. The assessment covered all key components of the project, including smart contract logic, access controls, and potential attack vectors. While no critical issues were found, we recommend ongoing security monitoring and best practices to maintain the integrity and resilience of the system.



# **Vulnerabilities High**

## Interface noncompliance: ERC5192 with transfer

Vulnerability severity: High

Contract claims to support ERC5192 interface while allowing transfer

Recommendations:

Remove transferFrom or remove IERC5192 from the supported interfaces list, noting this is then not truly souldbound



## **Vulnerabilities Medium**

## Missing existence check

Vulnerability severity: Medium

locked is missing an exitence check on tokenId

Recommendations:

Ensure tokenId represents a valid, existing token.



## **Vulnerabilities** Low

#### **Current scan criticals Clear**

During this scan no low security vulnerabilities were identified. The assessment covered all key components of the project, including smart contract logic, access controls, and potential attack vectors. While no critical issues were found, we recommend ongoing security monitoring and best practices to maintain the integrity and resilience of the system.



## **Vulnerabilities Info**

## **Unnecessary Storage Gap**

Vulnerability severity: Info

The contract is not upgradeable, but implements a storage gap

Recommendations:

Remove the storage gap

#### **Missing event**

Vulnerability severity: Info

mintfunction does not emit events.

Recommendations:

Ensure all state changing functions emit appropriate events.



#### **Disclaimer**

#### **Disclaimer**

This report is governed by the Fidesium terms and conditions.

This report does not constitute an endorsement or disapproval of any project or team, nor does it reflect the economic value or potential of any related product or asset. It is not investment advice and should not be used as the basis for investment decisions. Instead, this report provides an assessment intended to improve code quality and mitigate risks inherent in cryptographic tokens and blockchain technology.

Fidesium does not guarantee the absence of bugs or vulnerabilities in the technology assessed, nor does it comment on the business practices, models, or regulatory compliance of its creators. All services, reports, and materials are provided "as is" and "as available," without warranties of any kind, including but not limited to merchantability, fitness for a particular purpose, or non-infringement.

Cryptographic assets and blockchain technologies are novel and carry inherent technical risks, uncertainties, and the possibility of unpredictable outcomes. Assessment results may contain inaccuracies or depend on third-party systems, and reliance on them is solely at the Customer's risk.

Fidesium assumes no liability for content inaccuracies, personal injuries, property damages, or losses related to the use of its services, reports, or materials. Third-party components are provided "as is," and any warranties are strictly between the Customer and the third-party provider.

These services and materials are intended solely for the Customer's use and benefit. No third party or their representatives may claim rights to or rely on these services, reports, or materials under any circumstances.