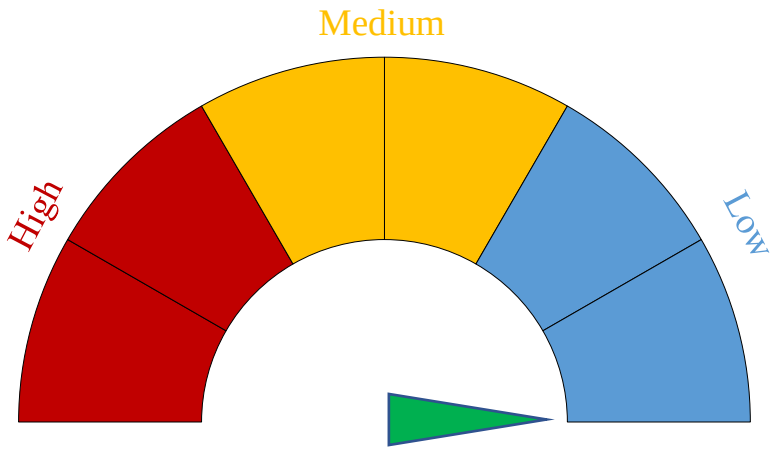
SECURICHAIN

SMART CONTRACT SECURITY ANALYSIS REPORT FOR

CATIA

May 16th 2024



RISK RATING

(Overall rating of SecuriChain based on the number and severity of detected issues)

Disclaimer

This report containing confidential information can be used internally by the Customer, or it can be disclosed publicly after all vulnerabilities are fixed — upon a decision of the Customer.

SecuriChain do not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed.

The reports in no way provide investment advice, nor should be leveraged as investment advice of any sort.

TABLE OF CONTENTS

1. VULNERABILITY ASSESSMENT OVERVIEW

1.1. ASSIGNING RISK LEVELS

Auditor categorizes each of the detected vulnerabilities into 4 levels (**High**, **Medium**, **Low**, and **Info**) according to the degree of the risks it may cause in Customer's operations. For details of the rating standards, please refer to "Appendix 2 Risk Rating." Please also note that the assessment of the findings is based on Auditor's own perspective and may contain speculations in some cases.

1.2. SCOPE OF WORK

Project Name	**CATIA**
Platform	Ethereum
Languages	Solidity
Methods	Automation Scan, Architecture Review, Functional Testing, Manual CODE Review
Repository	Commit: 66796e5
Documents	
Timelines	10/05/2024 – 16/05/2024

1.3. CHECKSUM FILE

STT	Hash	Name
1	2f78b1f3d0a5b74172da0e060ca79024c24d76dd16ee251a7c8300b15dea98e8	Pool.sol
2	d6bd31e080cde1da653b94a2cf353d3d537bc3d5dc9f810e15b89882f40d328d	FPEMap.sol
3	1033b81c9a2c3793467479bdef1c63f01dbbafceaf723811493d8e3b948d0475	Feistel.sol

1.4. ASSESSMENT RESULTS

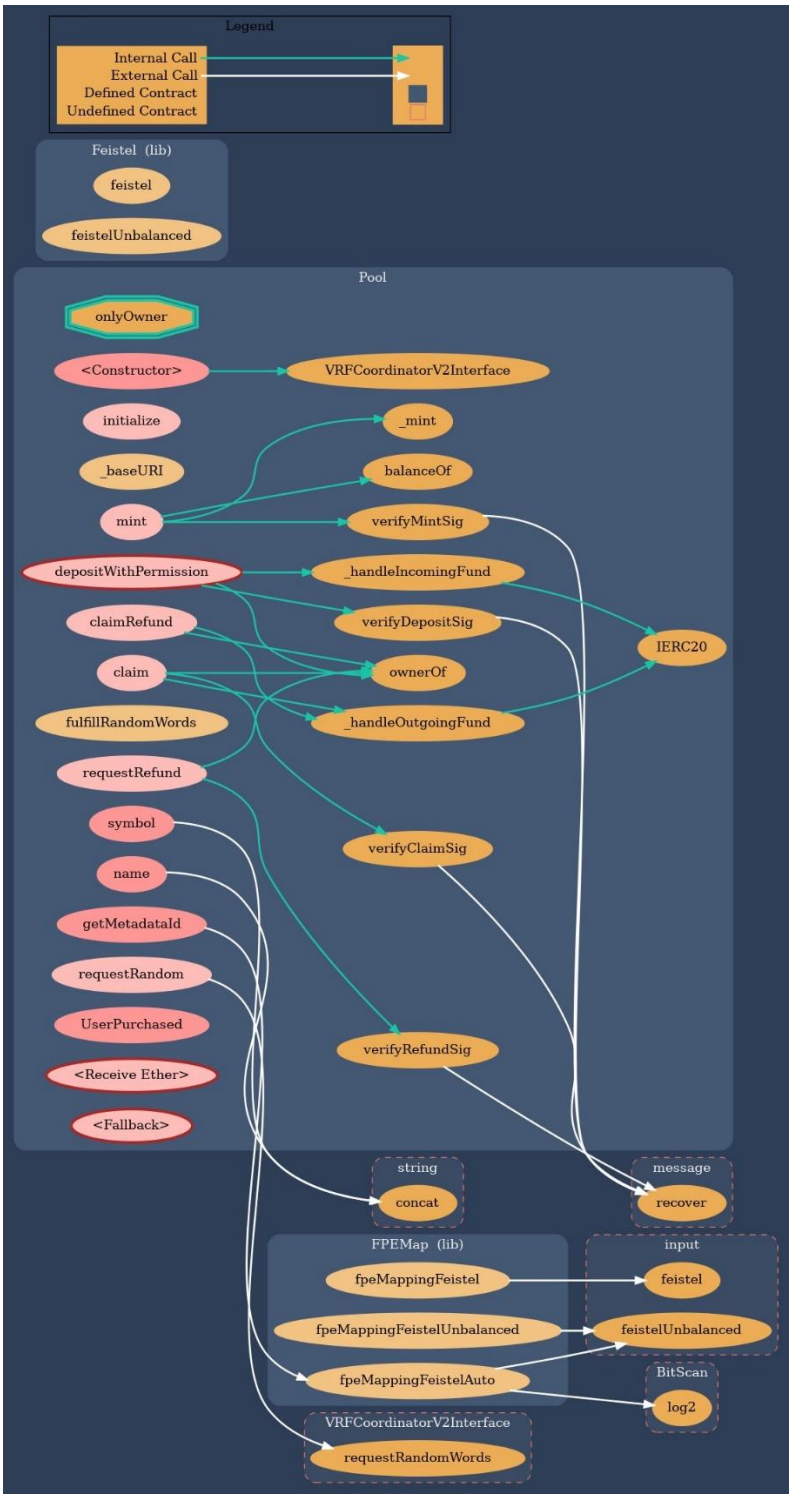
Grade "**A+**"- No vulnerability detected

Grade	Description
A+	Very secure environment with no vulnerability detected
A	**Low-**level vulnerability detected
B	**Medium**-level vulnerability detected
C	**High**-level vulnerability detected
D	Several different types of **High**-level vulnerabilities detected
*****	Unsubstantiated, possible vulnerability detected

(*For information on criteria for risk rating, refer to Appendix.2)*

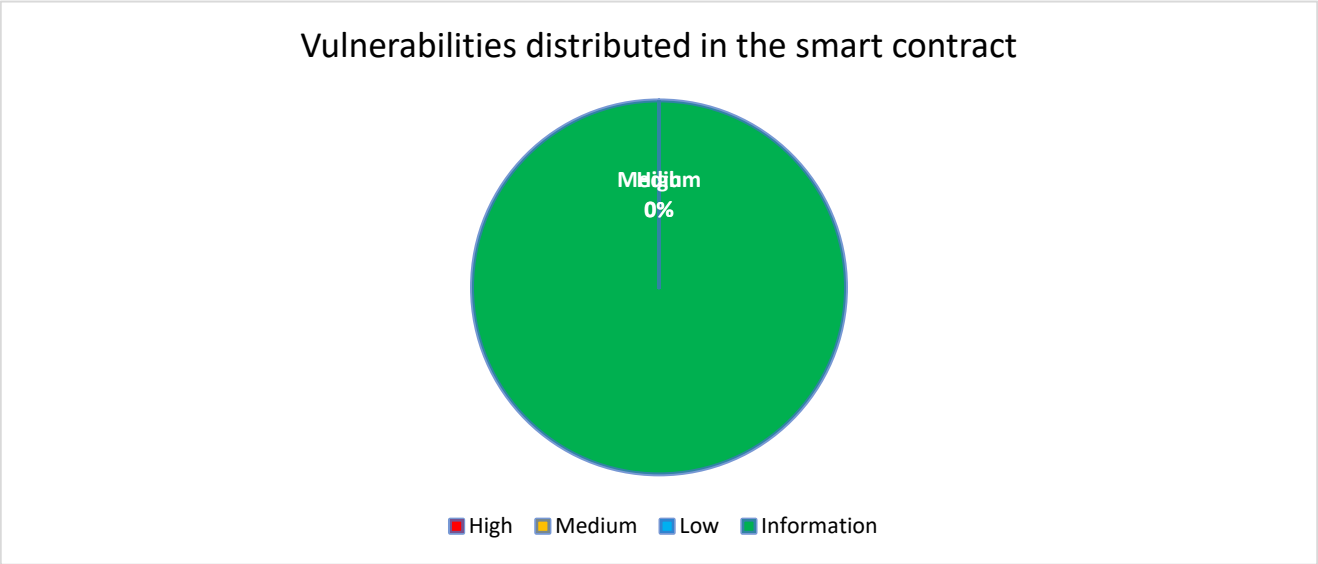
2. FINDINGS

2.1. CALL GRAPH



2.2. LIST OF VULNERABILITIES

The detected vulnerabilities are listed below. Please refer to "Appendix.2 Risk Rating" for the risk assessment method.



(For rating of each vulnerability, refer to Appendix 2.)

No vulnerability detected.

2.3. DETAILS

No vulnerability detected.

3. CONCLUSION

This document, and its appendices, represents our best effort to capture the results of several days of intensive activity. During that time, our consultants conducted extensive mapping activity, vulnerability detection, and exploitation from across the Internet.

Assessments such as this one are an important step in maintaining the security posture of these Internet-facing systems. If the recommendations given in this report are followed, the various system owners can be assured of having exercised due diligence towards protecting its computing assets.

Please feel free to direct any questions on this assessment to: audit@securichain.io

APPENDIX 1. ASSESSMENT LIST

CHECKLIST		
Arithmetic operations		
	Integer Overflow/Underflow	Integer Division
	Integer Truncation	Integer Sign
	Wrong Operator	
Re-entrancy		
Bad Randomness		
	Timestamp Dependence	Blockhash
Front running		
DDos		
	DOS By Complex Fallback Function	DOS By Gaslimit
	DOS By Non-existent Address Or Malicious Contract	
Unsafe external calls		
Gas usage		
	Invariants in Loop	Invariants State Variables Are Not Declared Constant
Business Logics Review		
Access Control & Authorization		
	Replay Attack	Use tx.origin For Authentication
Logic Vulnerability		

APPENDIX 2. RISK RATING

Risk Level	Explain	Example Types
High	The issue puts a large number of users' sensitive information at risk, or is reasonably likely to lead to catastrophic impact for client's reputation or serious financial implications for client and users.	Re-entrancy
		Front running
		DDos
		Bad Randomness
		Logic Vulnerability
		Arithmetic operations
Medium	The issue puts a subset of users' sensitive information at risk, would be detrimental for the client's reputation if exploited, or is reasonably likely to lead to moderate financial impact.	Access Control
		Unsafe external calls
		Business Logics Review
		Logic Vulnerability
Low	The risk is relatively small and could not be exploited on a recurring basis, or is a risk that the client has indicated is lowimpact in view of the client's business circumstances.	Gas usage
Info	The issue does not post an immediate risk, but is relevant to security best practices or Defence in Depth.	Do not specify a specific version of Solidity

