

**HACKEN**

# SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

Customer: RedFox

Date: November 8<sup>th</sup>, 2021

This document may contain confidential information about IT systems and the intellectual property of the Customer as well as information about potential vulnerabilities and methods of their exploitation.

The 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.

## Document

<b>Name</b>	Smart Contract Code Review and Security Analysis Report for RedFox.
<b>Approved by</b>	Andrew Matiukhin   CTO Hacken OU
<b>Type</b>	Bridge
<b>Platform</b>	Ethereum / Solidity
<b>Methods</b>	Architecture Review, Functional Testing, Computer-Aided Verification, Manual Review
<b>Repository</b>	<a href="https://github.com/RFL-Valt/eth-bridge-contract">https://github.com/RFL-Valt/eth-bridge-contract</a>
<b>Commit</b>	12b635b1a4425ee3cecd642b37423ddfadf8087b
<b>Technical Documentation</b>	NO
<b>JS tests</b>	YES
<b>Website</b>	redfoxlabs.io
<b>Timeline</b>	03 NOVEMBER 2021 - 08 NOVEMBER 2021
<b>Changelog</b>	08 NOVEMBER 2021 - Initial Audit



## Table of contents

Introduction	4
Scope	4
Executive Summary	5
Severity Definitions	7
Audit overview	8
Conclusion	11
Disclaimers	12

## Introduction

Hacken OÜ (Consultant) was contracted by RedFox (Customer) to conduct a Smart Contract Code Review and Security Analysis. This report presents the findings of the security assessment of the Customer's smart contract and its code review conducted between November 3<sup>rd</sup>, 2021 - November 8<sup>th</sup>, 2021.

## Scope

The scope of the project is smart contracts in the repository:

**Repository:**

<https://github.com/RFL-Valt/eth-bridge-contract>

**Commit:**

[12b635b1a4425ee3cecd642b37423ddfadf8087b](https://github.com/RFL-Valt/eth-bridge-contract/commit/12b635b1a4425ee3cecd642b37423ddfadf8087b)

**Technical Documentation:** No

**JS tests:** Yes (included in the repo: “/test/”)

**Contracts:**

[Verify.sol](#)  
[test/Token.sol](#)  
[ETHWAXBRIDGE.sol](#)  
[interfaces/ERC20Interface.sol](#)  
[Owned.sol](#)  
[libraries/Math.sol](#)  
[libraries/Endian.sol](#)

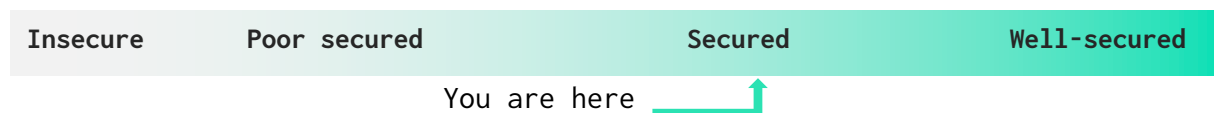
We have scanned this smart contract for commonly known and more specific vulnerabilities. Here are some of the commonly known vulnerabilities that are considered:

Category	Check Item
Code review	<ul style="list-style-type: none"><li>▪ Reentrancy</li><li>▪ Ownership Takeover</li><li>▪ Timestamp Dependence</li><li>▪ Gas Limit and Loops</li><li>▪ DoS with (Unexpected) Throw</li><li>▪ DoS with Block Gas Limit</li><li>▪ Transaction-Ordering Dependence</li><li>▪ Style guide violation</li><li>▪ Costly Loop</li><li>▪ ERC20 API violation</li><li>▪ Unchecked external call</li><li>▪ Unchecked math</li><li>▪ Unsafe type inference</li><li>▪ Implicit visibility level</li><li>▪ Deployment Consistency</li><li>▪ Repository Consistency</li><li>▪ Data Consistency</li></ul>

Functional review	<ul style="list-style-type: none"> <li>▪ Business Logics Review</li> <li>▪ Functionality Checks</li> <li>▪ Access Control &amp; Authorization</li> <li>▪ Escrow manipulation</li> <li>▪ Token Supply manipulation</li> <li>▪ Assets integrity</li> <li>▪ User Balances manipulation</li> <li>▪ Data Consistency manipulation</li> <li>▪ Kill-Switch Mechanism</li> <li>▪ Operation Trails &amp; Event Generation</li> </ul>
-------------------	---

## Executive Summary

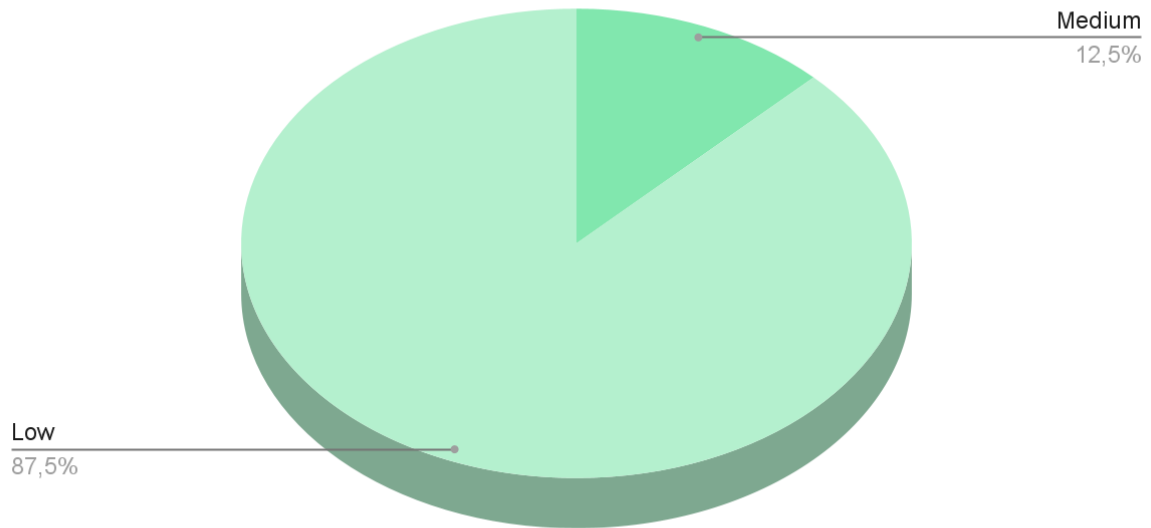
According to the assessment, the Customer's smart contracts are secured but not fully test-covered.



Our team performed an analysis of code functionality, manual audit, and automated checks with Mythril and Slither. All issues found during automated analysis were manually reviewed, and important vulnerabilities are presented in the Audit overview section. All found issues can be found in the Audit overview section.

As a result of the audit, security engineers found 1 medium and 7 low severity issues.

Graph 1. The distribution of vulnerabilities after the audit.



## Severity Definitions

Risk Level	Description
<b>Critical</b>	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
<b>High</b>	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions
<b>Medium</b>	Medium-level vulnerabilities are important to fix; however, they can't lead to assets loss or data manipulations.
<b>Low</b>	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution

## Audit overview

### Critical

No critical issues were found.

### High

No high severity issues were found.

### Medium

Very low tests coverage

The overall test coverage is about 31% for statements and 17% for code branches which is too low. Many aspects of the code and logic branches remain untested.

File	% Stmts	% Branch	% Funcs	% Lines	Uncovered Lines
contracts/	27.16	15.79	58.82	28.09	
ETHWAXBRIDGE.sol	25	10.71	54.55	25.37	... 279,280,282
Owned.sol	100	75	100	100	
Verify.sol	0	0	0	0	... 37,39,48,50
contracts/interfaces/	100	100	100	100	
ERC20Interface.sol	100	100	100	100	
contracts/libraries/	0	0	0	0	
Endian.sol	0	100	0	0	... 24,28,31,34
Math.sol	0	0	0	0	... 19,20,24,25
contracts/test/	43.04	22.22	36.11	41.46	
Token.sol	43.04	22.22	36.11	41.46	... 782,783,819
All files	31.64	17.07	38.33	31.38	

**Recommendation:** Please write more tests and ensure that you have covered the code for at least 95%.

### Low

1. Inconsistency of naming and declaring

The contract's name is set to "ERC20Interface" while it is not declared as an interface but an abstract contract.

**Contract:** ERC20Interface.sol

**Recommendation:** Fix inconsistency in the naming.

2. The imported contract was never used

While ETHWAXBRIDGE imports ERC20Interface but it never uses anything declared there.





**Contract:** ERC20Interface.sol

**Recommendation:** Remove excess import statement.

3. Missing events

**updateThreshold** has no event so it is hard to track these changes off-chain.

**Contract:** ETHWAXBRIDGE.sol

**Function:** updateThreshold

**Recommendation:** Please emit an event on threshold change.

4. Boolean equality

Boolean constants can be used directly and do not need to be compared to **true** or **false**.

**Contract:** Oracled.sol

**Functions:** unregOracle, onlyOracle

**Recommendation:** Remove the equality to the boolean constant.

5. A public function that could be declared external

**public** functions that are never called by the contract should be declared **external** to save gas.

**Contract:** ETHWAXBRIDGE.sol

**Functions:** receiveApproval, regOracle, unregOracle, bridge, claim, updateThreshold, transferAnyERC20Token

**Recommendation:** Use the **external** attribute for functions never called from the contract.

6. A public function that could be declared external

**public** functions that are never called by the contract should be declared **external** to save gas.

**Contract:** Owned.sol

**Functions:** transferOwnership, acceptOwnership

**Recommendation:** Use the **external** attribute for functions never called from the contract.

7. A public function that could be declared external

**public** functions that are never called by the contract should be declared **external** to save gas.

**Contract:** ERC20Interface.sol



**Functions:** totalSupply, balanceOf, allowance, transfer, approve, transferFrom

**Recommendation:** Use the **external** attribute for functions never called from the contract.



## Conclusion

Smart contracts within the scope were manually reviewed and analyzed with static analysis tools.

The audit report contains all found security vulnerabilities and other issues in the reviewed code.

As a result of the audit, security engineers found **1** medium and **7** low severity issues.



## Disclaimers

### **Hacken Disclaimer**

The smart contracts given for audit have been analyzed in accordance with the best industry practices at the date of this report, in relation to cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report (Source Code); the Source Code compilation, deployment, and functionality (performing the intended functions).

The audit makes no statements or warranties on the security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bug-free status, or any other statements of the contract. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only – we recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts.

### **Technical Disclaimer**

Smart contracts are deployed and executed on a blockchain platform. The platform, its programming language, and other software related to the smart contract can have vulnerabilities that can lead to hacks. Thus, the audit can't guarantee the explicit security of the audited smart contracts.