QuillAudits

Audit Report
February, 2024

For

onXRP

Table of Content

Scope of Audit

The scope of this audit was to analyze and document the Bidds-Contracts-Coreum codebase by onXRP for quality, security, and correctness.

Checked Vulnerabilities

- Re-entrancy
- Timestamp Dependence
- Transaction-Ordering Dependence
- Exception disorder
- Balance equality
- Malicious libraries
- Compiler version not fixed
- Redundant fallback function
- Style guide violation
- Unchecked math
- Unsafe type inference
- Implicit visibility level
- Correct liquidity on ticks

Techniques and Methods

Throughout the audit of smart contracts, care was taken to ensure:

- The overall quality of code.
- Use of best practices.
- Code documentation and comments match logic and expected behavior.
- Liquidity computation on ranged ticks are correct.

The following techniques, methods, and tools were used to review all the smart contracts.

Structural Analysis

In this step, we have analyzed the design patterns and structure of smart contracts. A thorough check was done to ensure the smart contract is structured in a way that will not result in future problems

Static Analysis

A static Analysis of Smart Contracts was done to identify contract vulnerabilities. In this step, a series of automated tools are used to test the security of smart contracts.

Code Review / Manual Analysis

Manual Analysis or review of code was done to identify new vulnerabilities or verify the vulnerabilities found during the static analysis. Code base were completely manually analyzed, their logic was checked and compared with the one described in the whitepaper. Besides, the results of the automated analysis were manually verified.

Issue Categories

Every issue in this report has been assigned to a severity level. There are four levels of severity, and each of them has been explained below.

High Severity Issues

A high severity issue or vulnerability means that your smart contract can be exploited. Issues on this level are critical to the smart contract's performance or functionality, and we recommend these issues be fixed before moving to a live environment.

Medium Severity Issues

The issues marked as medium severity usually arise because of errors and deficiencies in the smart contract code. Issues on this level could potentially bring problems, and they should still be fixed.

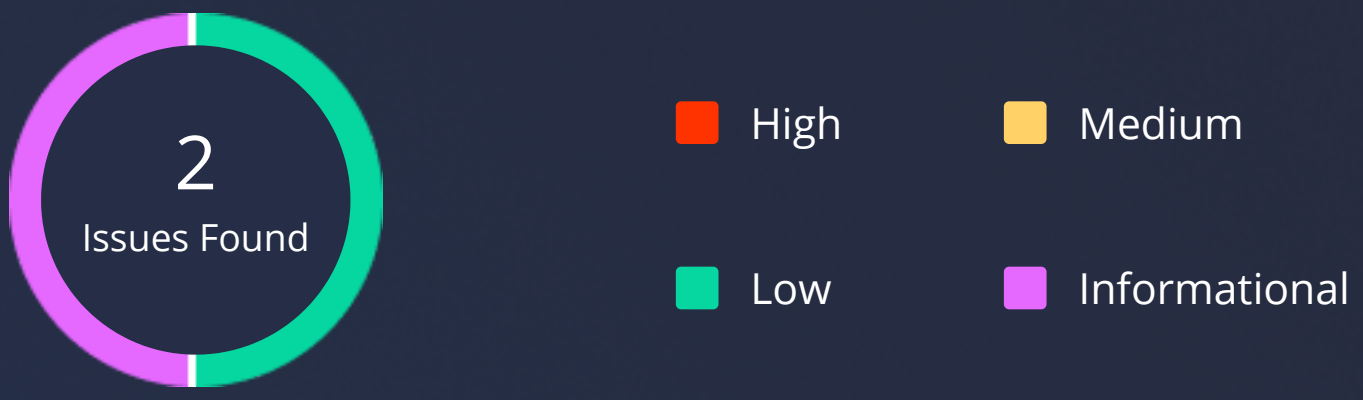
Low Severity Issues

Low-level severity issues can cause minor impact and or are just warnings that can remain unfixed for now. It would be better to fix these issues at some point in the future.

Informational Issues

These are four severity issues that indicate an improvement request, a general question, a cosmetic or documentation error, or a request for information. There is low-to-no impact.

Number of Security Issues per Severity



	High	Medium	Low	Informational
Open Issues	0	0	0	0
Acknowledged Issues	0	0	0	0
Partially Resolved Issues	0	0	0	0
Resolved Issues	0	0	1	1

Introduction

On **Jan 18, 2024** - QuillAudits Team performed a security audit for **Bidds-Contracts-Coreum** smart contracts(onXRP).

The code for the audit was taken from following the official link:

https://github.com/onxrp-insights/Bidds-Contracts-Coreum

Version Number	Date	Commit ID	Files
01	Dec 29	a8661003898884298 7d552f4f0b4f71f50a23fdb	/*
01	Jan 2	79b3ad0b8ed503aeee71771aef0e9b7429474641	/*
01	Jan 16	10bc249fa62506b37d06819daedbc1607eeba4b7	/*
01	Feb 6	129b4fe3d1716074f70886d0164bb96056c4d0f1	/*
01	Feb 6	44a6b2f47af4921604b2a253070021b9ec4ede5a	/*

A. Bidds-Contracts-Coreum

Issues Found – Code Review / Manual Testing

Low Severity Issues

A.1 Test Suite is failing and no coverage report

Description

The test suite exhibits a failure of executing tests, indicating issues. Additionally, the absence of a coverage report implies a lack of information regarding test coverage.

Remediation

To rectify this issue, the recommended steps involve resolving the failing test cases and integrating a library such as **cargo-llvm-cov or tarpaulin** to generate a comprehensive coverage report.

Status

Resolved

Informational Issues

A.2 Lack of CIs on Repository

Description

The repository ought to incorporate Continuous Integrations (CIs), specifically for the execution of the test suite, generation of coverage reports, and enforcement of code linting.

Remediation

Implement a minimum set of pipelines within the integration framework, encompassing distinct stages for test suite execution, coverage report generation with a mandated threshold exceeding 95% for branch coverage, and code linting like **dylint.**

Status

Resolved

Automated Tests

Dylint:

No major issues were found. Some false positive errors were reported by the tool. All the other issues have been categorized above according to their level of severity

Closing Summary

No instances of Integer Overflow and Underflow vulnerabilities are found in the contract.

As recommended, the Bidds team(onXRP Team) has gone through the above-mentioned details and fixed the code.

Disclaimer

QuillAudits Smart contract security audit provides services to help identify and mitigate potential security risks in **Bidds-Contracts-Coreum(onXRP)** smart contracts. However, it is important to understand that no security audit can guarantee complete protection against all possible security threats. QuillAudits audit reports are based on the information provided to us at the time of the audit, and we cannot guarantee the accuracy or completeness of this information. Additionally, the security landscape is constantly evolving, and new security threats may emerge after the audit has been completed.

Therefore, it is recommended that multiple audits and bug bounty programs be conducted to ensure the ongoing security of **Bidds-Contracts-Coreum(onXRP)** smart contracts. One audit is not enough to guarantee complete protection against all possible security threats. It is important to implement proper risk management strategies and stay vigilant in monitoring your smart contracts for potential security risks.

QuillAudits cannot be held liable for any security breaches or losses that may occur subsequent to and despite using our audit services. It is the responsibility of the **Bidds-Contracts-Coreum(onXRP)** to implement the recommendations provided in our audit reports and to take appropriate steps to mitigate potential security risks.

About QuillAudits

QuillAudits is a secure smart contracts audit platform designed by QuillHash Technologies. We are a team of dedicated blockchain security experts and smart contract auditors determined to ensure that Smart Contract-based Web3 projects can avail the latest and best security solutions to operate in a trustworthy and risk-free ecosystem.

1000+
Audits Completed

$30B
Secured

800K
Lines of Code Audited

Follow Our Journey

Audit Report
February, 2024

For

onXRP

QuillAudits

Canada, India, Singapore, UAE, UK

www.quillaudits.com

audits@quillhash.com