«project-name» Security Review

Version «version-number»

«current-date»

Conducted by:
«researcher-name», Independent Security Researcher

Table of Contents

1 About «researcher-name»

«researcher-introduction»

2 Disclaimer

Audits are a time, resource and expertise bound effort where trained experts evaluate smart contracts using a combination of automated and manual techniques to find as many vulnerabilities as possible. Audits can show the presence of vulnerabilities **but not their absence**.

3 Risk classification

Severity	Impact: High	Impact: Medium	Impact: Low
Likelihood: High	Critical	High	Medium
Likelihood: Medium	High	Medium	Low
Likelihood: Low	Medium	Low	Low

3.1 Impact

- **High** - leads to a significant loss of assets in the protocol or significantly harms a group of users.
- **Medium** - only a small amount of funds can be lost or a functionality of the protocol is affected.
- **Low** - any kind of unexpected behaviour that's not so critical.

3.2 Likelihood

- **High** - direct attack vector; the cost is relatively low to the amount of funds that can be lost.
- **Medium** - only conditionally incentivized attack vector, but still relatively likely.
- **Low** - too many or too unlikely assumptions; provides little or no incentive.

3.3 Actions required by severity level

- **Critical** - client **must** fix the issue.
- **High** - client **must** fix the issue.
- **Medium** - client **should** fix the issue.
- **Low** - client **could** fix the issue.

4 Executive summary

Overview

Project Name	«project-name»
Repository	«project-repository»
Commit hash	«review-hash»
Resolution	«resolution-hash»
Methods	Manual review

Scope

«relative-path-1»
«relative-path-2»
«relative-path-3»

Issues Found

Governance risk	88
Critical risk	«c»
High risk	«h»
Medium risk	«m»
Low risk	«l»
Informational	«i»

5 Findings

5.1 Governance risk

5.1.1 «title-governance-1»

Severity: *Governance risk*

Context: «relative-path-governance-1»

Description: «description-governance-1»

Recommendation: «recommendation-governance-1»

Resolution: «resolution-governance-1»

5.2 Critical risk

5.2.1 «title-critical-1»

Severity: *Critical risk*

Context: «relative-path-critical-1»

Description: «description-critical-1»

Recommendation: «recommendation-critical-1»

Resolution: «resolution-critical-1»

5.3 High risk

5.3.1 «title-high-1»

Severity: *High risk*

Context: «relative-path-high-1»

Description: «description-high-1»

Recommendation: «recommendation-high-1»

Resolution: «resolution-high-1»

5.4 Medium risk

5.4.1 «title-medium-1»

Severity: *Medium risk*

Context: «relative-path-medium-1»

Description: «description-medium-1»

Recommendation: «recommendation-medium-1»

Resolution: «resolution-medium-1»

5.5 Low risk

5.5.1 «title-low-1»

Severity: *Low risk*

Context: «relative-path-low-1»

Description: «description-low-1»

Recommendation: «recommendation-low-1»

Resolution: «resolution-low-1»

5.6 Informational

5.6.1 «title-informational-1»

Severity: *Informational*

Context: «relative-path-informational-1»

Description: «description-informational-1»

Recommendation: «recommendation-informational-1»

Resolution: «resolution-informational-1»