CYBERULTRON CONSULTING
PRIVATE LIMITED

Smart Contract Code Review Report

22 June 2022

Version: 1.0

Table Of Content

Overview

The Security Code Audit of Smart Contract of Gov-Contracts started on 15th June 2022 and ended on 24th June 2022.

Methodology

The code audit is carried out using the specification of CWE (Common Weakness Enumeration) Guidelines laid down by the community. The code audit also included some elements of manual testing.

Findings Overview

There was a total of 2 vulnerabilities identified in the contracts. Following is their distribution.

- 1 Medium Vulnerability

Finding Details

MEDIUM - Improper Errors handling

Severity

MEDIUM

Contract Name/s

List of Contracts Affected

- contracts.rs

Category

- Improper implementation of Error Logging
- Insufficient Logging

CWE Reference

- CWE-778 Insufficient logging

Description

In **execute_refund** & **execute_slash** function in contracts.rs the error returns always return the same error returns "**NonPassedProposalRefund"** while the actual reason for error returns can be multiple. (i.e. - Failure due to veto, active proposal etc)

Reason this would be a issue if a contracts calls for execute_refund it would be very difficult to debug at to what caused the call to fail.

Code Reference/s

contracts.rs - Multiple lines - 476:5716

Remediation

Assign errors for all the states of execution independently.