Bastet

Smart Contract Audit Report

一張含有 卡通, 符號, 藝術, 貓頭鷹 的圖片

自動產生的描述

**About Bastet**

Bastet is a comprehensive dataset of common smart contract vulnerabilities in DeFi along with an AI-driven automated detection process to enhance vulnerability detection accuracy and optimize security lifecycle management.

**Risk Classification**

|  |  |  |  |
| --- | --- | --- | --- |
| Severity Level | Impact: High | Impact: Medium | Impact: Low |
| Likelihood: High | High | Medium | Low |
| Likelihood: Medium | Medium | Low | Informational |
| Likelihood: Low | Low | Informational | Informational |

**Impact**

* **High:** leads to a loss of assets in the protocol, or significant harm to majority of users.
* **Medium:** function or availability of the protocol could be impacted or losses to only a subset of users.
* **Low:** State handling, function incorrect as to spec, issues with clarity, losses will be annoying but bearable.

**Likelihood**

* **High:** almost certain to happen, easy to perform, or not easy but highly incentivized.
* **Medium:** only conditionally possible or incentivized, but still relatively likely.
* **Low:** requires stars to align, or little-to-no incentive.

**Security Assessment Summary**

This security assessment is supported by [Bastet](https://github.com/OneSavieLabs/Bastet). Bastet is an AI vulnerability detection infrastructure that includes a dataset of common DeFi smart contract vulnerabilities as well as multiple vulnerability detection processes. It can identify medium- to high-risk issues observed on-chain and in past audit competitions and, through its customizable detection workflows, improves the accuracy of automated vulnerability discovery. Bastet also supports comprehensive security evaluations during development, auditing, and monitoring phases.

**Project Summary**

**File in Scope:** {{file\_name}}

**Issues Found:**

|  |  |
| --- | --- |
| **Severity** | **Count** |
| High | {{severity\_counts.high}} |
| Medium | {{severity\_counts.medium}} |
| Low | {{severity\_counts.low}} |
| Informational | {{severity\_counts.informational}} |
| **Total** | {{total\_vulnerabilities}} |

**Findings**

|  |  |
| --- | --- |
| {%tr for vuln in vulnerabilities %} | |
| Summary | {{ vuln.summary }} |
| Severity | {{ vuln.severity}} |
| Discription | {{ vuln.vulnerability}} |
| Recommendation | {{ vuln.recommendation}} |
|  | |
| {%tr endfor %} | |