Smart Contract Security Analysis Report

Repository Information

Repository: eth-infinitism/account-abstraction
Files Analyzed: 46
Analysis Tool: SMCVD (Smart Contract Vulnerability Detector)
Date: 2025-09-29

Executive Summary

The analysis of the eth-infinitism/account-abstraction repository identified 3 medium-severity vulnerabilities. The overall risk level is assessed as **medium**.

Note: AI-enhanced detailed analysis was not available due to API quota limitations.

Risk Assessment

Overall Risk Level: Medium

Vulnerabilities by Severity:

Severity	Count
Medium	3

Identified Vulnerabilities

1. Timestamp Dependence

Severity: Medium
File: EntryPoint.sol (Line 426)
Confidence: 0.90
Description: Reliance on block timestamp for critical operations
Impact: Manipulation of time-based logic, unfair advantages
Recommendation: Avoid using block.timestamp for critical logic, use block numbers

2. Unchecked External Call

Severity: Medium
File: EntryPoint.sol (Line 165)
Confidence: 0.80
Description: External call without checking return value
Impact: Silent failures, unexpected behavior
Recommendation: Always check return values of external calls

3. Timestamp Dependence

Severity: Medium
File: StakeManager.sol (Line 72)
Confidence: 0.81
Description: Reliance on block timestamp for critical operations
Impact: Manipulation of time-based logic, unfair advantages
Recommendation: Avoid using block.timestamp for critical logic, use block numbers

Recommendations

1. Address Timestamp Dependencies: Replace block.timestamp usage with more secure alternatives where possible.
2. Implement Return Value Checks: Ensure all external calls check their return values and handle failures appropriately.
3. Conduct Manual Security Review: Perform a thorough manual review of the identified vulnerabilities.
4. Upgrade OpenAI Plan: Consider upgrading your OpenAI plan to enable full AI-enhanced analysis capabilities.

Conclusion

The eth-infinitism/account-abstraction repository shows good security practices overall but has some medium-severity issues that should be addressed. The identified vulnerabilities are not critical but could be exploited under certain conditions. Addressing these issues will improve the overall security posture of the smart contracts.