
SECURITY ANALYSIS REPORT (SAR)

Project: Analysis Request 1063

Based on: Snapshot 891

Tools used: Scout Scan

2024-04-15_19-52

○ Disclaimer

This report is not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any “product” created by any team that contracts TestMachine. This report is based on the scope of materials and documentation provided to TestMachine. Results may not be complete nor inclusive of all vulnerabilities. This report does not provide any warranty or guarantee regarding the absolute product, software or services or that such will be bug-free, without risk or subject to vulnerabilities nature of the technology analyzed.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides financial or investment advice, nor should be leveraged as financial or investment advice of any sort. TestMachine's position is that each company and individual are responsible for their own due diligence and continuous security. TestMachine's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies.

⬡ Analyzed Files

 OmronDeposit.sol







○ Results Summary

There is 1 vulnerable file out of a total of 1 analyzed in your solidity project. The vulnerability with the most occurrences is "Block values as a proxy for time" which has a medium severity. This vulnerability appears 3 times in the project. Additionally, there are vulnerabilities of low severity related to an "Outdated Compiler Version" which appear 2 times.

There are also informational vulnerabilities regarding "Unprotected Functions Using RBAC" which appear 5 times. These informational vulnerabilities may not pose an immediate threat but should still be addressed to ensure the security of your project.

Overall, the project needs attention to address these vulnerabilities. While the low severity vulnerabilities can be easily fixed, the medium severity vulnerabilities may require more effort and time to resolve. It is crucial to allocate resources to fix these vulnerabilities promptly to ensure the overall security of the project.

Totals by Severity

Severity	Count
 High	0
 Medium	3
 Low	1
 Informational	5
 Optimization	0
 Unknown	0

Totals by Tool

Tool	Count
Scout Scan	9

Findings from tool: Scout Scan

medium

Block values as a proxy for time [TMR-017](#)

uploaded/891/OmronDeposit.sol:419:420

Found error: block.timestamp in _calculatePointsDiff. Found 3 time-related warnings:. Using block values like 'block.timestamp' and 'block.number' as a proxy for time is risky as they are not precise and can be manipulated to some extent.

Recommendation

It's recommended to use oracles or other external time services for more precise time-keeping.

medium

Block values as a proxy for time [TMR-017](#)

uploaded/891/OmronDeposit.sol:404:405

Found error: block.timestamp in _updatePoints. Found 3 time-related warnings:. Using block values like 'block.timestamp' and 'block.number' as a proxy for time is risky as they are not precise and can be manipulated to some extent.

Recommendation

It's recommended to use oracles or other external time services for more precise time-keeping.

medium

Block values as a proxy for time [TMR-017](#)

uploaded/891/OmronDeposit.sol:160:161

Found error: block.timestamp in stopDeposits. Found 3 time-related warnings:. Using block values like 'block.timestamp' and 'block.number' as a proxy for time is risky as they are not precise and can be manipulated to some extent.

Recommendation

It's recommended to use oracles or other external time services for more precise time-keeping.

low

Outdated Compiler Version [TMR-003](#)

uploaded/891/OmronDeposit.sol:1:1

Found error: Full Inliner Non Expression Split Argument Evaluation Order. Compiler 0.8.21 may introduce bugs.. undefined

Recommendation

Please upgrade to a version without these issues.

informational

Unprotected Functions Using RBAC [TMR-038](#)

uploaded/891/OmronDeposit.sol:419:420

Found error: _calculatePointsDiff. Found 5 unprotected functions using RBAC:. Unprotected functions using RBAC can lead to unauthorized access.

Recommendation

Review the functions to ensure they have the appropriate access controls applied.

informational

Unprotected Functions Using RBAC [TMR-038](#)

uploaded/891/OmronDeposit.sol:275:276

Found error: tokenBalance. Found 5 unprotected functions using RBAC:. Unprotected functions using RBAC can lead to unauthorized access.

Recommendation

Review the functions to ensure they have the appropriate access controls applied.

informational

Unprotected Functions Using RBAC [TMR-038](#)

uploaded/891/OmronDeposit.sol:262:263

Found error: calculatePoints. Found 5 unprotected functions using RBAC:. Unprotected functions using RBAC can lead to unauthorized access.

Recommendation

Review the functions to ensure they have the appropriate access controls applied.

informational


Unprotected Functions Using RBAC [TMR-038](#)

uploaded/891/OmronDeposit.sol:249:250

Found error: getAllWhitelistedTokens. Found 5 unprotected functions using RBAC:. Unprotected functions using RBAC can lead to unauthorized access.

Recommendation

Review the functions to ensure they have the appropriate access controls applied.

 informational

Unprotected Functions Using RBAC [TMR-038](#)

uploaded/891/OmronDeposit.sol:228:229

Found error: getUserInfo. Found 5 unprotected functions using RBAC:. Unprotected functions using RBAC can lead to unauthorized access.

Recommendation

Review the functions to ensure they have the appropriate access controls applied.

Security Analysis Report (SAR) provided by



<https://testmachine.ai>