GA GUARDIAN

M0

M0 M-Portal-Lite

Security Assessment

August 15th, 2025

Summary

Audit Firm Guardian

Prepared By Cosine, Osman Ozdemir, Curiousapple, Vladamir Zotov

Client M0

Final Report Date August 15, 2025

Audit Summary

M0 engaged Guardian to review the security of their M0 M-Portal-Lite. From the 11th of August to the 12th of August, a team of 4 auditors reviewed the source code in scope. All findings have been recorded in the following report.

Confidence Ranking

Given the lack of critical issues detected and minimal code changes following the main review, Guardian assigns a Confidence Ranking of 5 to the protocol. Guardian advises the protocol to consider periodic review with future changes. For detailed understanding of the Guardian Confidence Ranking, please see the rubric on the following page.

🔗 Blockchain network: **Ethereum, Arbitrum, Optimism, Linea**

✅ Verify the authenticity of this report on Guardian's GitHub: https://github.com/guardianaudits

📊 Code coverage & PoC test suite: https://github.com/GuardianOrg/m-portal-lite-mportallite-team1

Guardian Confidence Ranking

Confidence Ranking	Definition and Recommendation	Risk Profile
5: Very High Confidence	Codebase is mature, clean, and secure. No High or Critical vulnerabilities were found. Follows modern best practices with high test coverage and thoughtful design. **Recommendation:** Code is highly secure at time of audit. Low risk of latent critical issues.	0 High/Critical findings and few Low/Medium severity findings.
4: High Confidence	Code is clean, well-structured, and adheres to best practices. Only Low or Medium-severity issues were discovered. Design patterns are sound, and test coverage is reasonable. Small changes, such as modifying rounding logic, may introduce new vulnerabilities and should be carefully reviewed. **Recommendation:** Suitable for deployment after remediations; consider periodic review with changes.	0 High/Critical findings. Varied Low/Medium severity findings.
3: Moderate Confidence	Medium-severity and occasional High-severity issues found. Code is functional, but there are concerning areas (e.g., weak modularity, risky patterns). No critical design flaws, though some patterns could lead to issues in edge cases. **Recommendation:** Address issues thoroughly and consider a targeted follow-up audit depending on code changes.	1 High finding and ≥ 3 Medium. Varied Low severity findings.
2: Low Confidence	Code shows frequent emergence of Critical/High vulnerabilities (~2/week). Audit revealed recurring anti-patterns, weak test coverage, or unclear logic. These characteristics suggest a high likelihood of latent issues. **Recommendation:** Post-audit development and a second audit cycle are strongly advised.	2-4 High/Critical findings per engagement week.
1: Very Low Confidence	Code has systemic issues. Multiple High/Critical findings (≥5/week), poor security posture, and design flaws that introduce compounding risks. Safety cannot be assured. **Recommendation:** Halt deployment and seek a comprehensive re-audit after substantial refactoring.	≥5 High/Critical findings and overall systemic flaws.

Table of Contents

Project Overview

Project Summary

Project Name	M0
Language	Solidity
Codebase	https://github.com/m0-foundation/m-portal-lite
Commit(s)	Initial commit: ae5baef7d5cbbc326b65b8be92a38d2eebb5c3b4 Final commit: ae5baef7d5cbbc326b65b8be92a38d2eebb5c3b4

Audit Summary

Delivery Date	August 15, 2025
Audit Methodology	Static Analysis, Manual Review, Test Suite, Contract Fuzzing

Vulnerability Summary

Vulnerability Level	Total	Pending	Declined	Acknowledged	Partially Resolved	Resolved
Critical	0	0	0	0	0	0
High	0	0	0	0	0	0
Medium	1	0	0	1	0	0
Low	1	0	0	1	0	0
Info	2	0	0	2	0	0

Audit Scope & Methodology

Scope:
m-portal-lite/commit-ae5baef/src/Portal.sol

Audit Scope & Methodology

Vulnerability Classifications

Severity	Impact: *High*	Impact: *Medium*	Impact: *Low*
Likelihood: *High*	🔴 Critical	🟠 High	🟡 Medium
Likelihood: *Medium*	🟠 High	🟡 Medium	🟢 Low
Likelihood: *Low*	🟡 Medium	🟢 Low	🟢 Low

Impact

High Significant loss of assets in the protocol, significant harm to a group of users, or a core functionality of the protocol is disrupted.

Medium A small amount of funds can be lost or ancillary functionality of the protocol is affected. The user or protocol may experience reduced or delayed receipt of intended funds.

Low Can lead to any unexpected behavior with some of the protocol's functionalities that is notable but does not meet the criteria for a higher severity.

Likelihood

High The attack is possible with reasonable assumptions that mimic on-chain conditions, and the cost of the attack is relatively low compared to the amount gained or the disruption to the protocol.

Medium An attack vector that is only possible in uncommon cases or requires a large amount of capital to exercise relative to the amount gained or the disruption to the protocol.

Low Unlikely to ever occur in production.

Audit Scope & Methodology

Methodology

Guardian is the ultimate standard for Smart Contract security. An engagement with Guardian entails the following:

- Two competing teams of Guardian security researchers performing an independent review.
- A dedicated fuzzing engineer to construct a comprehensive stateful fuzzing suite for the project.
- An engagement lead security researcher coordinating the 2 teams, performing their own analysis, relaying findings to the client, and orchestrating the testing/verification efforts.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross-referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts. Comprehensive written tests as a part of a code coverage testing suite.
- Contract fuzzing for increased attack resilience.

Findings & Resolutions

ID	Title	Category	Severity	Status
M-01	Happy Path: Normal Users Would Receive M Tokens	Logical Error	Medium	Acknowledged
L-01	Error Path : Normal User May Receive M Tokens	Validation	Low	Acknowledged
I-01	Incorrect Comment	Informational	Info	Acknowledged
I-02	Earning Cannot Be Re-Enabled Once Disabled	Warning	Info	Acknowledged

M-01 | Happy Path: Normal Users Would Receive M Tokens

Category	Severity	Location	Status
Logical Error	Medium	Portal.sol: 312-313	Acknowledged

Description

The original intent for the M token was to be permissionless, allowing anyone to hold it. However, based on recent discussions with the M0 team, the model has changed:

• New intent: Only selected role holders are allowed to handle the native M token directly.
• Regular users should instead interact with M extensions (wrapped versions of M) for DeFi and other use cases.

However, the current Portal implementation does not reflect this new intent. If the destination token in a spoke/hub transfer is set to the native M token address, the Portal will issue or transfer native M tokens directly.

• The `swapInM` function in the Swap Facility only allows approved swappers to swap native M into wrapped M.
• This means users who receive native M cannot wrap it themselves.
• Since wrapped M is the expected token for DeFi integrations, users would be stuck holding the native token, unable to use it in the intended ecosystem.

Under M0's original (permissionless) deployment assumptions, this flow was fine. But with the new restricted model, this scenario can occur even in the `happy path`.

Example:

• On Mainnet Hub (`0x36f586A30502AE3afb555b8aA4dCc05d233c2ecE`), the destination token for Linea is currently set to native M.
• As a result, if a user calls `transfer` on the Portal, they receive native M on Linea instead of the wrapped version.

Recommendation

Set the default destination token to the wrapped M (`wM`) instead of native M, so that by default:
• The Portal wraps into `wM` before delivering to the user.
• If a different extension specified, wrap into that instead.

Resolution

M0 Team: Acknowledged. This is acceptable behavior and will be addresses by configuration of approved bridging paths for Portals.

L-01 | Error Path : Normal User May Receive M Tokens

Category	Severity	Location	Status
Validation	● Low	Portal.sol: 339-345	Acknowledged

Description

When a user makes a cross chain transfer with a M extension token the flow looks like this:

• On the source chain the `swapOutM` function is called to convert the M extension tokens to $M tokens
• The $M tokens are transferred to the destination chain
• On the destination chain the system tries to wrap the $M tokens to M extension tokens with the `swapInM` function
• But in case the `swapInM` call fails the user just receives the $M tokens instead

This is problematic as normal users should never receive $M tokens and as a normal user is not able to use the `swapInM` function the user might not be able to do anything with these tokens.

A malicious actor might also be able to do this on purpose (in case the actor sees any benefit of doing so).

For example if the M extension token has a minimum amount restriction for the wrap function of $100 the user could perform multiple $99.99 cross chain transfers to load himself up with $M tokens.

Recommendation

Consider leaving the tokens inside the contract or transferring them to another one and let an admin handle the situation if this edge case occurs.

Resolution

M0 Team: Acknowledged. This is acceptable behavior for now.

I-01 | Incorrect Comment

Category	Severity	Location	Status
Informational	Info	SpokePortal.sol: 128	Acknowledged

Description

The comment above the `_revertIfUnsupportedDestinationChain` function on line 128 of `SpokePortal` contract is incorrect. It should be: "Reverts if the destination chain is not the Hub chain".

Recommendation

Update the comment.

Resolution

M0 Team: Acknowledged. Will fix.

I-02 | Earning Cannot Be Re-Enabled Once Disabled

Category	Severity	Location	Status
Warning	Info	HubPortal.sol: 200-201	Acknowledged

Description

The `_isEarningEnabled` function is implemented as:

```
function _isEarningEnabled() internal view returns (bool) {

    return wasEarningEnabled & disableEarningIndex = IndexingMath.EXP_SCALED_ONE;

}
```

Given this logic:

Once `disableEarningIndex` is set to current Index in `disableEarning`, earning can not be enabled again.

Recommendation

Be aware of this constraint.

Resolution

M0 Team: Acceptable behavior.

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” or “asset” created by any team or project that contracts Guardian to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

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 investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. Guardian’s position is that each company and individual are responsible for their own due diligence and continuous security. Guardian’s goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by Guardian is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

Notice that smart contracts deployed on the blockchain are not resistant from internal/external exploit. Notice that active smart contract owner privileges constitute an elevated impact to any smart contract’s safety and security. Therefore, Guardian does not guarantee the explicit security of the audited smart contract, regardless of the verdict.

About Guardian

Founded in 2022 by DeFi experts, Guardian is a leading audit firm in the DeFi smart contract space. With every audit report, Guardian upholds best-in-class security while achieving our mission to relentlessly secure DeFi.

To learn more, visit https://guardianaudits.com

To view our audit portfolio, visit https://github.com/guardianaudits

To book an audit, message https://t.me/guardianaudits