GA GUARDIAN

# M0

## M0 M-Extensions

## Security Assessment

August 15th, 2025

# Summary

**Audit Firm** Guardian

**Prepared By** Curiousapple, Wafflemakr, Cosine, Osman Ozdemir, Vladamir Zotov

**Client** M0

**Final Report Date** August 15, 2025

## Audit Summary

M0 engaged Guardian to review the security of their M0 M-Extensions. From the 8th of August to the 11th of August, a team of 5 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**

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

📊 PoC test suite: https://github.com/GuardianOrg/m-extensions-m0-m-extensions-team1

https://github.com/GuardianOrg/m-extensions-m0-m-extensions-team2

https://github.com/GuardianOrg/m-extensions-m0-m-extensions-fuzz

# 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.<br><br>**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.<br><br>**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.<br><br>**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.<br><br>**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.<br><br>**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-extensions |
| Commit(s) | Initial commit: 90f144deee35071e02b1ff0b62004b8d2435ddfe<br>Final commit: 011f84f0f6a701a9796fcac1ad29896c60b65344 |

## 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 | 0 | 0 | 1 |
| Low | 0 | 0 | 0 | 0 | 0 | 0 |
| Info | 1 | 0 | 0 | 0 | 0 | 1 |

# Audit Scope & Methodology

```
contract,source,total,comment
evm-m-extensions-90f144d/src/MExtension.sol,86,262,123
evm-m-extensions-90f144d/src/libs/IndexingMath.sol,32,97,51
evm-m-extensions-90f144d/src/components/Freezable.sol,67,151,53
evm-m-extensions-90f144d/src/components/IFreezable.sol,8,51,33
evm-m-extensions-90f144d/src/projects/yieldToOne/IMYieldToOne.sol,8,38,20
evm-m-extensions-90f144d/src/projects/yieldToOne/MYieldToOne.sol,113,263,94
evm-m-extensions-90f144d/src/projects/yieldToAllWithFee/MSpokeYieldFee.sol,20,75,43
evm-m-extensions-90f144d/src/projects/yieldToAllWithFee/MYieldFee.sol,263,535,154
evm-m-extensions-90f144d/src/swap/ReentrancyLock.sol,45,84,15
evm-m-extensions-90f144d/src/swap/SwapFacility.sol,149,319,98
evm-m-extensions-90f144d/src/swap/UniswapV3SwapAdapter.sol,135,256,72
evm-m-extensions-90f144d/src/projects/earnerManager/IMEarnerManager.sol,17,82,46
evm-m-extensions-90f144d/src/projects/earnerManager/MEarnerManager.sol,256,519,152
source count: {
  total: 2732,
  source: 1199,
  comment: 954,
  single: 295,
  block: 659,
  mixed: 0,
  empty: 580,
  todo: 0,
  blockEmpty: 1,
  commentToSourceRatio: 0.7956630525437864
}
```

# 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.

# Invariants Assessed

During Guardian's review of M0, fuzz-testing was performed on the protocol's main functionalities. Given the dynamic interactions and the potential for unforeseen edge cases in the protocol, fuzz-testing was imperative to verify the integrity of several system invariants.

Throughout the engagement the following invariants were assessed for a total of 10,000,000+ runs with a prepared fuzzing suite.

| ID | Description | Tested | Passed | Remediation | Run Count |
|---|---|---|---|---|---|
| MYF-01 | MYieldFee extension mToken Balance must be greater or equal than projectedSupply | ✅ | ❌ | ❌ | 10M+ |
| MYF-02 | MYieldFee extension mToken Balance must be greater or equal than projectedSupply + fee | ✅ | ❌ | ❌ | 10M+ |
| SWAP-01-00 | YTO-TO-YTO: MYieldToOne yield must not change after swaps | ✅ | ✅ | ✅ | 10M+ |
| SWAP-01-01 | YFEE-TO-YFEE: MYieldFee yield must not change after swaps | ✅ | ✅ | ✅ | 10M+ |
| SWAP-01-02 | MEARN-TO-MEARN: MEarnerManager yield must not change after swaps | ✅ | ✅ | ✅ | 10M+ |
| SWAP-02 | Swap facility M0 balance must be 0 after swap out | ✅ | ✅ | ✅ | 10M+ |
| SWAP-03 | Total M0 balance of all users must not change after swap | ✅ | ✅ | ✅ | 10M+ |
| SWAP-04 | Received amount of M0 must be greater or equal than slippage | ✅ | ✅ | ✅ | 10M+ |
| SWAP-05 | Received amount of USDC must be greater or equal than slippage | ✅ | ✅ | ✅ | 10M+ |

# Invariants Assessed

| ID | Description | Tested | Passed | Remediation | Run Count |
|---|---|---|---|---|---|
| MEARN-01 | MEarnerManager extension mToken Balance must be greater or equal than projectedTotalSupply | ✅ | ❌ | ✅ | 10M+ |
| ERR-01 | Unexpected Error | ✅ | ✅ | ✅ | 10M+ |

# Findings & Resolutions

| ID | Title | Category | Severity | Status |
|---|---|---|---|---|
| M-01 | Irreversible Permission Flags | Access Control | Medium | Acknowledged |
| I-01 | Redundant Checks In swapWithPermit | Superfluous Code | Info | Acknowledged |

# M-01 | Irreversible Permission Flags

| Category | Severity | Location | Status |
| --- | --- | --- | --- |
| Access Control | Medium | SwapFacility.sol: 193-194 | Resolved |

## Description

Once an extension is set as permissioned via `setPermissionedExtension`, it cannot be made permissionless again due to an early return in the function.

Similarly, once an M swapper is allowed via `setPermissionedMSwapper`, they cannot be disallowed. This prevents role or permission revocation, which could lead to security and governance limitations.

## Recommendation

Consider allowing permission flags to be toggled in both directions.

## Resolution

M0 Team: The issue was resolved in PR#47.

# I-01 | Redundant Checks In swapWithPermit

| Category | Severity | Location | Status |
| --- | --- | --- | --- |
| Superfluous Code | Info | SwapFacility.sol: 112-116 | Resolved |

## Description

One of the `swapWithPermit` functions in the `SwapFacility` contract checks if the given extensions are approved and not permissioned before calling the `_swap` function which does the same.

## Recommendation

Consider removing the redundant checks.

## Resolution

M0 Team: The issue was resolved in PR#48.

# 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