THREE SIGMA

M0 M-Extensions ERC20 Token

Security Review

M^0

Disclaimer

Security Review

M0 M-Extensions ERC20 Token

Disclaimer

The ensuing audit offers no assertions or assurances about the code's security. It cannot be deemed an adequate judgment of the contract's correctness on its own. The authors of this audit present it solely as an informational exercise, reporting the thorough research involved in the secure development of the intended contracts, and make no material claims or guarantees regarding the contract's post-deployment operation. The authors of this report disclaim all liability for all kinds of potential consequences of the contract's deployment or use. Due to the possibility of human error occurring during the code's manual review process, we advise the client team to commission several independent audits in addition to a public bug bounty program.

Table of Contents

Security Review

M0 M-Extensions ERC20 Token

Table of Contents

Summary

Security Review

M0 M-Extensions ERC20 Token

Summary

Three Sigma audited M0 M-Extensions in a 2.4 person week engagement. The audit was conducted from 28/04/2025 to 05/05/2025.

Protocol Description

M0 M-Extensions allows users to wrap M Tokens into a stable, fixed-balance token while keeping the interest generated by the underlying M Token. The key feature is that all yield earned by the wrapped tokens is claimable by a single designated recipient, not distributed to token holders.

Scope

Security Review

M0 M-Extensions ERC20 Token

Scope

Filepath	nSLOC
src/abstract/MExtension.sol	118
src/abstract/components/Blacklistable.sol	64
src/USDHL.sol	114
Total	296

Methodology

Security Review

M0 M-Extensions ERC20 Token

Methodology

To begin, we reasoned meticulously about the contract's business logic, checking security-critical features to ensure that there were no gaps in the business logic and/or inconsistencies between the aforementioned logic and the implementation. Second, we thoroughly examined the code for known security flaws and attack vectors. Finally, we discussed the most catastrophic situations with the team and reasoned backwards to ensure they are not reachable in any unintentional form.

Taxonomy

In this audit, we classify findings based on Immunefi's Vulnerability Severity Classification System (v2.3) as a guideline. The final classification considers both the potential impact of an issue, as defined in the referenced system, and its likelihood of being exploited. The following table summarizes the general expected classification according to impact and likelihood; however, each issue will be evaluated on a case-by-case basis and may not strictly follow it.

Impact / Likelihood	LOW	MEDIUM	HIGH
NONE	None		
LOW	Low		
MEDIUM	Low	Medium	Medium
HIGH	Medium	High	High
CRITICAL	High	Critical	Critical

Project Dashboard

Security Review

M0 M-Extensions ERC20 Token

Project Dashboard

Application Summary

Name	M0 M-Extensions
Repository	https://github.com/felixprotocol/m-extensions
Commit	12442fa
Language	Solidity
Platform	Ethereum

Engagement Summary

Timeline	28/04/2025 to 05/05/2025
№ of Auditors	2
Review Time	2.4 person weeks

Vulnerability Summary

Issue Classification	Found	Addressed	Acknowledged
Critical	0	0	0
High	0	0	0
Medium	0	0	0
Low	0	0	0
None	0	0	0

Category Breakdown

Suggestion	0
Documentation	0
Bug	0
Optimization	0
Good Code Practices	0

Risk Section

Security Review

M0 M-Extensions ERC20 Token

Risk Section

No risks identified.

Findings

Security Review

M0 M-Extensions ERC20 Token

Findings

No findings identified.