Mori Protocol
Audit Report

Tue Dec 19 2023

contact@scalebit.xyz https://twitter.com/scalebit_

ScaleBit

Mori Protocol Audit Report

1 Executive Summary

1.1 Project Information

Description	A concentrated liquidity swap protocol.
Type	Dex
Auditors	ScaleBit
Timeline	Tue Dec 12 2023 - Tue Dec 19 2023
Languages	Solidity
Platform	Viction
Methods	Architecture Review, Unit Testing, Manual Review
Source Code	https://github.com/mori-protocol/mori-contracts
Commits	1df8d84b031aec3afda19baaf3d73f17a8aa6730 7d1819b565b05f534aa9fbf26cef72882d89adf7

1.2 Files in Scope

The following are the SHA1 hashes of the original reviewed files.

ID	File	SHA-1 Hash
TIC	projects/v3-core/contracts/libraries/Tick.sol	37ef664ced74a41e7a2f438cdbf99527566f1aab
LGSM	projects/v3-core/contracts/libraries/LowGasSafeMath.sol	1bee2d0f85bc054e3b63a7e92c67d237a49c650c
SCA	projects/v3-core/contracts/libraries/SafeCast.sol	c3b25ed7fa205de6cc2075d96e27908d43f21671
FP9	projects/v3-core/contracts/libraries/FixedPoint96.sol	3a3ab5c10385c523c1738b9eb9d86dcd5f59c3f4
POS	projects/v3-core/contracts/libraries/Position.sol	0d6be19a8ba07321743fc90010a969b0fe26e301
FMA	projects/v3-core/contracts/libraries/FullMath.sol	0c531e95498282fc6ad5856e6273b7675b15bea0
SMA	projects/v3-core/contracts/libraries/SwapMath.sol	585ec272ca9a5a9b5d4645178b64fb52003e6091
ORA	projects/v3-core/contracts/libraries/Oracle.sol	49519e7e73e076479b04d0027d342468126e4cba
LMA	projects/v3-core/contracts/libraries/LiquidityMath.sol	2d440d1d862d4612b08243581f9232887b489c09
FP1	projects/v3-core/contracts/libraries/FixedPoint128.sol	22517ba8d668bb4e86a45f3f29ed077d72fb7608
THE	projects/v3-core/contracts/libraries/TransferHelper.sol	09f4e335c7ed41383bf2f04bf278169218994fc8

TBI	projects/v3-core/contracts/libraries/TickBitmap.sol	f14dad9bee719bffd0bd7fc54d2da37f289561d8
TMA	projects/v3-core/contracts/libraries/TickMath.sol	7eee6a798a068e6eaaa63ce8f432ee193e0ff2e0
UMA	projects/v3-core/contracts/libraries/UnsafeMath.sol	d3e3ff1ab78e03ccec335ab6da4ea76b578cb422
BMA	projects/v3-core/contracts/libraries/BitMath.sol	82ee70afdc183819ee3705d274a506a42f1e278b
SPM	projects/v3-core/contracts/libraries/SqrtPriceMath.sol	0bf7a6c27c88689b4ade289bf0683adabe90a570
TRSO	projects/v3-periphery/contracts/libraries/TokenRatioSortOrder.sol	84ff0b5257a032c234bf53b3866a857edd30512b
PAT	projects/v3-periphery/contracts/libraries/Path.sol	2504b1a543392240bddbe04efef9c47cecdc704b
CID	projects/v3-periphery/contracts/libraries/ChainId.sol	a2ffce157a73a5b87024ed2bb54f9c3ae19b04c3
HST	projects/v3-periphery/contracts/libraries/HexStrings.sol	fc19854bf736b050ab6a78bb595cef7a43699b45
THE	projects/v3-periphery/contracts/libraries/TransferHelper.sol	6cedc556d3cf7b972f78e7c64670ebfbd7f4c9cc
BLI	projects/v3-periphery/contracts/libraries/BytesLib.sol	747be1412bfe71b5c06f4bbfa7cb7b2c968bfdcc
PKE	projects/v3-periphery/contracts/libraries/PositionKey.sol	6cc88dd5fd105faa25c6f048b0e7da4e50263c8b
IMU	projects/v3-periphery/contracts/interfaces/IMulticall.sol	9e6b62357fe6d6748e7a5c4765c6ae6e1d732632

IERC2M	projects/v3-periphery/contracts/interfaces/IERC20Metadata.sol	907ee3f5af9e65dd1c6d0fc44e4faee11f8204f6
IQU	projects/v3-periphery/contracts/interfaces/IQuoter.sol	2788a5a0905543bd5aadc4d3ff36ef7e40a105a1
IERC7P	projects/v3-periphery/contracts/interfaces/IERC721Permit.sol	ebae2281a1a29f8039994e45ae290dcc11cfd35e
IPI	projects/v3-periphery/contracts/interfaces/IPoolInitializer.sol	5e91f53e858852ce1ce70f623f869c8976a0fe53
ISP	projects/v3-periphery/contracts/interfaces/ISelfPermit.sol	fb8db7a56077ca32dd58a4a9bc25b54e2ad57071
INTPD	projects/v3-periphery/contracts/interfaces/INonfungibleTokenPositionDescriptor.sol	1b2a07a417f71dd9b40e9fd376ad0ec00660c3ad
IPPWF	projects/v3-periphery/contracts/interfaces/IPeripheryPaymentsWithFee.sol	0da1ac6c52abfdbc8171d40f3ee898e08818cb31
ITL	projects/v3-periphery/contracts/interfaces/ITickLens.sol	5bb2a6b9e8f948f1d9ffb60f7d93ed7e72eecfd3
IERC2PA	projects/v3-periphery/contracts/interfaces/external/IERC20PermitAllowed.sol	0f8ae33f339095b7745444ede48774f4023f7b0e
IERC1	projects/v3-periphery/contracts/interfaces/external/IERC1271.sol	5560885f1e908f592046013d4df11ca12416d522
IWETH9	projects/v3-periphery/contracts/interfaces/external/IWETH9.sol	4d0d313953cb956315e444b9d94b8ccc27c3d99f
MUL	projects/v3-periphery/contracts/base/Multicall.sol	e48264609451e31ffea549e7db3e30815080505c

BTI	projects/v3-periphery/contracts/base/BlockTimestamp.sol	e9433e812b02a43ae225b797863e5102e802ef27
PPA	projects/v3-periphery/contracts/base/PeripheryPayments.sol	ba48c46d36b30ed6efcb5809b92eb422d49f3f2d
ERC7P	projects/v3-periphery/contracts/base/ERC721Permit.sol	402f58139a0bdc704f6b5737075454601084dc9c
PVA	projects/v3-periphery/contracts/base/PeripheryValidation.sol	078495af30569dfdb02365ae8340f54d03b04c96
SPE	projects/v3-periphery/contracts/base/SelfPermit.sol	bea7d24d2f467a5ad0a34d9d07c2b0e868506fc6
PIS	projects/v3-periphery/contracts/base/PeripheryImmutableState.sol	238ba15bdc60250ead1a2f21c8307d175c9d0880
NTPDOC	projects/v3-periphery/contracts/NonfungibleTokenPositionDescriptorOffChain.sol	29c8fdc6b1d4cabc2a07a7b187d7e67a85687647
SCA	projects/masterchef-v3/contracts/libraries/SafeCast.sol	0cd843e1c910d1119af2322434690839ebf09547
MUL	projects/masterchef-v3/contracts/utils/Multicall.sol	8137902e1c2215f98bd78d6e5a49752945133822
INPM	projects/masterchef-v3/contracts/interfaces/INonfungiblePositionManager.sol	4726560f70c49cad3758333d06ae1323dd62ac41
INPMS	projects/masterchef-v3/contracts/interfaces/INonfungiblePositionManagerStruct.sol	0dbc51143791c3bece7803f279890b447eebf90f
IMCV3	projects/masterchef-v3/contracts/interfaces/IMasterChefV3.sol	864a959be1fb257c2e82f4b6c76407dfba49f01a

IWETH	projects/masterchef-v3/contracts/interfaces/IWETH.sol	766eb86ea7875d05ff6bd9f27bb24c3bc062c91e
IFB	projects/masterchef-v3/contracts/interfaces/IFarmBooster.sol	26a71a196d1e85f0a13929473d44cbc7a381d4a6
ENU	projects/masterchef-v3/contracts/Enumerable.sol	3d4bcab22971615ffb50b69501cef461608db671
IDV3F	projects/v3-core/contracts/interfaces/IDojoV3Factory.sol	65cd760aa716b366df552cce7437a1586e5b698e
IERC2M	projects/v3-core/contracts/interfaces/IERC20Minimal.sol	b51c0ea9c07a1cfa8cc4da9f02b4d8211d364d15
IDV3FC	projects/v3-core/contracts/interfaces/callback/IDojoV3FlashCallback.sol	195401d84be881dd5e87b867fa44105d50c72000
IDV3MC	projects/v3-core/contracts/interfaces/callback/IDojoV3MintCallback.sol	f167f2398a974ff41a6663dce5484725c560cb2f
IDV3SC	projects/v3-core/contracts/interfaces/callback/IDojoV3SwapCallback.sol	294d33920f63ca804b51dbd96151d59dd6709aaa
IDV3PD	projects/v3-core/contracts/interfaces/IDojoV3PoolDeployer.sol	a5f015c6ee74112043bf612d226ae8f79efc4ace
IDV3PI	projects/v3-core/contracts/interfaces/pool/IDojoV3PoolImmutables.sol	741034adf6b762fed38c5836d3462bade07fc8ad
IDV3PDS	projects/v3-core/contracts/interfaces/pool/IDojoV3PoolDerivedState.sol	6df0daba5a61bf8050cedfb6339b1729e037de56
IDV3PS	projects/v3-core/contracts/interfac	b15468ecb601ef5c2ed335227fe8c

	es/pool/IDojoV3PoolState.sol	17cfdd152a7
IDV3PE	projects/v3-core/contracts/interfaces/pool/IDojoV3PoolEvents.sol	7cd94a7c5117da47e9477913f84a8dc8bbe5b95e
IDV3PA	projects/v3-core/contracts/interfaces/pool/IDojoV3PoolActions.sol	728a1b480df3025fbe22b2f8aeeaec702ccbe2d8
IDV3POA	projects/v3-core/contracts/interfaces/pool/IDojoV3PoolOwnerActions.sol	cca71f7dbdbfc58aac57576ef8899aabfb5288ae
IDV3P	projects/v3-core/contracts/interfaces/IDojoV3Pool.sol	6fa9985cf5f11a00133fa685a1e9134afbd4d69b
DV3P	projects/v3-core/contracts/DojoV3Pool.sol	705eb30d0e4d27654edf1498946f440be9a8b50b
DV3F	projects/v3-core/contracts/DojoV3Factory.sol	b966e1699680fa30814ac847c0aae851ec06e798
DV3PD	projects/v3-core/contracts/DojoV3PoolDeployer.sol	c1cb280b96ea7fc467846093465c933b281b0e7e
DV3F1	projects/v3-core/DojoV3Factory.sol	02c5219ff8eb3a4bb02ca874c164f6e60e863023
LAM	projects/v3-periphery/contracts/libraries/LiquidityAmounts.sol	05a1df95cad917bcfd2c2e45b6434b2839127d46
OLI	projects/v3-periphery/contracts/libraries/OracleLibrary.sol	c25208dde16be7567eab75809f6eb02d3f03476c
PVA	projects/v3-periphery/contracts/libraries/PositionValue.sol	a0df1b2535b52293cf63cfe699f44d0463f65021
SPMP	projects/v3-periphery/contracts/libraries/SqrtPriceMathPartial.sol	a7549e24606feb6199ee07ca24dce97402c28e24

NFTD	projects/v3-periphery/contracts/libraries/NFTDescriptor.sol	d37753a5e3e8e5942f6f4585b43fe96f96d47306
NFTSVG	projects/v3-periphery/contracts/libraries/NFTSVG.sol	f4d901660f2f44f8d026d13f231d46f9b9d33f3c
CVA	projects/v3-periphery/contracts/libraries/CallbackValidation.sol	835d113888954ae6cff99b20cface93f60ed81d1
PTC	projects/v3-periphery/contracts/libraries/PoolTicksCounter.sol	7d6d14192e59952a3b16b6dfc1867a375ad5e2ab
PAD	projects/v3-periphery/contracts/libraries/PoolAddress.sol	2fb9a07cbefa166f7df7d5e6f2fa98ff7f523101
QUO	projects/v3-periphery/contracts/lens/Quoter.sol	e6bbd5d7880f27f36eaf5a55288d48f2f97e517d
TLE	projects/v3-periphery/contracts/lens/TickLens.sol	8849fe597df12e6fa12d82fa8e1a9718728eb806
DIM	projects/v3-periphery/contracts/lens/DojoInterfaceMulticall.sol	20b0ef3c4238c722ed7e7eeb7c90ab8e2f50dc0f
NPM	projects/v3-periphery/contracts/NonfungiblePositionManager.sol	e7f369dd43f355238a5117c0e63c93f07087f220
NFTDE	projects/v3-periphery/contracts/NFTDescriptorEx.sol	255aecd4b9994ff3d68bd2cef02ceb2137524859
INPM	projects/v3-periphery/contracts/interfaces/INonfungiblePositionManager.sol	1fd74f061fc2f8ea12d39344e60a3c1eb3f192e7
IPP	projects/v3-periphery/contracts/interfaces/IPeripheryPayments.sol	15b2eec9e5bd0b7c30a53f70480df8c452d6c2ef
ISR	projects/v3-periphery/contracts/interfaces/ISwapRouter.sol	423c8ebef30d6696997910ea141e21e7fc13f020

IV3M	projects/v3-periphery/contracts/interfaces/IV3Migrator.sol	f5f335fe8ff45131fc992e688f14fe445bc52ea9
IPIS	projects/v3-periphery/contracts/interfaces/IPeripheryImmutableState.sol	a44e911122fd2ef8a297b8eb0e2b2bdb483cf239
SRO	projects/v3-periphery/contracts/SwapRouter.sol	4d3faaba3dd3d01e27aaa863959906fb753c332b
NTPD	projects/v3-periphery/contracts/NonfungibleTokenPositionDescriptor.sol	70b2555e5d1c15f3b64c5703f9d0a0b8d999b5d2
PFL	projects/v3-periphery/contracts/examples/PairFlash.sol	7a674b0fa2f90966d3983bf4191e6db2bea290c4
LMA1	projects/v3-periphery/contracts/base/LiquidityManagement.sol	88c3c025e7792698abc7e561d72fec0b7985b527
PIN	projects/v3-periphery/contracts/base/PoolInitializer.sol	fa882826e2aba96ffe8718f38dcf338fb66464fc
PPWF	projects/v3-periphery/contracts/base/PeripheryPaymentsWithFee.sol	5a2b487e66c80a54fe1c6e80b224f54682e144b9
THE2	projects/masterchef-v3/contracts/libraries/TransferHelper.sol	7e5dfe7c4f58bafff0b92bfaa1196df7e2502925
IDV3P1	projects/masterchef-v3/contracts/interfaces/IDojoV3Pool.sol	683fffb31b6a66f70fbde2b2842fcb10e85612ad
IVA	projects/masterchef-v3/contracts/interfaces/IVault.sol	26913c915d2aff4634035a80cbb85fbfcfe1d441
ILMP	projects/masterchef-v3/contracts/interfaces/ILMPool.sol	1117a9b3d7aae5f39af35feb6c57a9ac50efd338
ILMPD	projects/masterchef-v3/contracts/i	2e73b482469e7dbdaa7318c15f0a

	nterfaces/ILMPoolDeployer.sol	9699661abe41
MCV3	projects/masterchef-v3/contracts/MasterChefV3.sol	a20d468d099106e2700b91235681bda1c8aa3a28
VAU	projects/masterchef-v3/contracts/Vault.sol	09dfa94511c402dedea7165fb2fa05c98cbf9866
DV3LPD	projects/v3-lm-pool/contracts/DojoV3LmPoolDeployer.sol	41633e715916f221a28612a07dd7eadd705da4de
LTI	projects/v3-lm-pool/contracts/libraries/LmTick.sol	af8bfbf3e44c23e0573fa002599ed2b2288a9b63
IMCV31	projects/v3-lm-pool/contracts/interfaces/IMasterChefV3.sol	246558f2fba9d4903cf36efda483a67eec154956
IDV3LP	projects/v3-lm-pool/contracts/interfaces/IDojoV3LmPool.sol	3ab9f303142819ba40a659810e107a5758948373
DV3LP	projects/v3-lm-pool/contracts/DojoV3LmPool.sol	d3222b4ffa798a0ee1956904ed706f22cd978948

1.3 Issue Statistic

Item	Count	Fixed	Acknowledged
Total	3	3	0
Informational	1	1	0
Minor	1	1	0
Medium	0	0	0
Major	1	1	0
Critical	0	0	0

1.4 ScaleBit Audit Breakdown

ScaleBit aims to assess repositories for security-related issues, code quality, and compliance with specifications and best practices. Possible issues our team looked for included (but are not limited to):

- Transaction-ordering dependence
- Timestamp dependence
- Integer overflow/underflow
- Number of rounding errors
- Unchecked External Call
- Unchecked CALL Return Values
- Functionality Checks
- Reentrancy
- Denial of service / logical oversights
- Access control
- Centralization of power
- Business logic issues
- Gas usage
- Fallback function usage
- tx.origin authentication
- Replay attacks
- Coding style issues

1.5 Methodology

The security team adopted the **"Testing and Automated Analysis"**, **"Code Review"** and **"Formal Verification"** strategy to perform a complete security test on the code in a way that is closest to the real attack. The main entrance and scope of security testing are stated in the conventions in the "Audit Objective", which can expand to contexts beyond the scope according to the actual testing needs. The main types of this security audit include:

(1) Testing and Automated Analysis

Items to check: state consistency / failure rollback / unit testing / value overflows / parameter verification / unhandled errors / boundary checking / coding specifications.

(2) Code Review

The code scope is illustrated in section 1.2.

(3) Audit Process

- Carry out relevant security tests on the testnet or the mainnet;
- If there are any questions during the audit process, communicate with the code owner in time. The code owners should actively cooperate (this might include providing the latest stable source code, relevant deployment scripts or methods, transaction signature scripts, exchange docking schemes, etc.);
- The necessary information during the audit process will be well documented for both the audit team and the code owner in a timely manner.

2 Summary

This report has been commissioned by Mori Protocol to identify any potential issues and vulnerabilities in the source code of the Mori Protocol smart contract, as well as any contract dependencies that were not part of an officially recognized library. In this audit, we have utilized various techniques, including manual code review and static analysis, to identify potential vulnerabilities and security issues.

During the audit, we identified 3 issues of varying severity, listed below.

ID	Title	Severity	Status
ILM-1	Lack of Events Emit	Minor	Fixed
MCV-1	Lack `indexed` In Event	Informational	Fixed
VAU-1	Vault `emergencyWithdraw` Design Issue	Major	Fixed

3 Participant Process

Here are the relevant actors with their respective abilities within the Mori Protocol Smart Contract:

Admin

- The Admin can set the statue of the pool through `setEmergency`.
- The Admin can set the receiver address through `setReceiver`.
- The Admin can set the LMPoolDeployer address through `setLMPoolDeployer`.
- The Admin can set the operatorAddress address through `setOperator`.
- The Admin can add a new farm pool through `add`.
- The Admin can update the pool's `REWARD` allocation point and `PeriodDuration`, `FarmBooster` address and through `set`, `setPeriodDuration` and `updateFarmBoostContract`.

User

- The User can open a position and get `lp` Token through `mint`.
- The User can increase the liquidity of his position through `increaseLiquidity`.
- The User can decrease the liquidity of his position through `decreaseLiquidity`.
- The User can collect the reward of his position through `collect`.
- The User can deposit their farm pool LP NFT to for staking and get reward through transfer NFT to `MasterChef`.
- The User can withdraw LP tokens from pool through `withdraw`.
- The User can update the liquidity of their NFT position through `updateLiquidity` / `increaseLiquidity` / `decreaseLiquidity`.
- If the User wants to quit the staking he can burn his LP NFT through `burn`.

4 Findings

ILM-1 Lack of Events Emit

Severity: Minor

Status: Fixed

Code Location:

projects/masterchef-v3/contracts/interfaces/ILMPool.sol#66

Descriptions:

The smart contract lacks appropriate events for monitoring sensitive operations, which could make it difficult to track sensitive actions or detect potential issues.

Suggestion:

It is recommended to emit events for those sensitive functions.

Resolution:

The client followed the suggestion and fixed this issue.

MCV-1 Lack `indexed` In Event

Severity: Informational

Status: Fixed

Code Location:

projects/masterchef-v3/contracts/MasterChefV3.sol#153-155

Descriptions:

Index event fields make the field more quickly accessible to off-chain tools that parse events. However, note that each index field costs extra gas during emission, so it's not necessarily best to index the maximum allowed per event (three fields). Each event should use three indexed fields if there are three or more fields and gas usage is not particularly of concern for the events in question. If there are fewer than three fields, all of the fields should be indexed.

Suggestion:

It is recommended to add `indexed` modifier in the event.

Resolution:

The client followed the suggestion and fixed this issue.

VAU-1 Vault `emergencyWithdraw` Design Issue

Severity: Major

Status: Fixed

Code Location:

projects/masterchef-v3/contracts/Vault.sol#28-42

Descriptions:

In the `emergencyWithdraw` function if the `_token` address is equal to `WETH`, the `amount` is calculated by `address(this).balance`. However, `WETH` is still an ERC20 Token, which doesn't get the correct amount of `WETH` owned by the contract in this way, resulting in `WETH` not being withdrawn correctly.

Suggestion:

It is recommended to fix this issue and changes to correct the transfer logic.

Resolution:

The client followed the suggestion and fixed this issue.

Appendix 1

Issue Level

- **Informational** issues are often recommendations to improve the style of the code or to optimize code that does not affect the overall functionality.
- **Minor** issues are general suggestions relevant to best practices and readability. They don't post any direct risk. Developers are encouraged to fix them.
- **Medium** issues are non-exploitable problems and not security vulnerabilities. They should be fixed unless there is a specific reason not to.
- **Major** issues are security vulnerabilities. They put a portion of users' sensitive information at risk, and often are not directly exploitable. All major issues should be fixed.
- **Critical** issues are directly exploitable security vulnerabilities. They put users' sensitive information at risk. All critical issues should be fixed.

Issue Status

- **Fixed:** The issue has been resolved.
- **Partially Fixed:** The issue has been partially resolved.
- **Acknowledged:** The issue has been acknowledged by the code owner, and the code owner confirms it's as designed, and decides to keep it.

Appendix 2

Disclaimer

This report is based on the scope of materials and documents provided, with a limited review at the time provided. Results may not be complete and do not include all vulnerabilities. The review and this report are provided on an as-is, where-is, and as-available basis. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your own risk. A report does not imply an endorsement of any particular project or team, nor does it guarantee its security. These reports should not be relied upon in any way by any third party, including for the purpose of making any decision to buy or sell products, services, or any other assets. TO THE FULLEST EXTENT PERMITTED BY LAW, WE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, IN CONNECTION WITH THIS REPORT, ITS CONTENT, RELATED SERVICES AND PRODUCTS, AND YOUR USE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NOT INFRINGEMENT.