Taker Swap
Audit Report

Mon Jan 06 2025

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

ScaleBit

Taker Swap Audit Report

1 Executive Summary

1.1 Project Information

Description	The Taker swap is a decentralized exchange
Type	DeFi
Auditors	ScaleBit
Timeline	Fri Dec 20 2024 - Mon Jan 06 2025
Languages	Solidity
Platform	Taker
Methods	Architecture Review, Unit Testing, Manual Review
Source Code	https://github.com/takerprotocol/taker-swap-contract
Commits	8655bde892c556018a4bc65a580746f8d3532210

1.2 Files in Scope

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

ID	File	SHA-1 Hash
TV3P	projects/v3-core/contracts/TakerV3Pool.sol	922ac4f7741ce0f5366a621dd028877a3f8f5fdd
TV3PD	projects/v3-core/contracts/TakerV3PoolDeployer.sol	375e11eccb68201e0d6c8f2cc9aa8e04ef39456a
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
TV3F	projects/v3-core/contracts/TakerV3Factory.sol	b8d475e9551d3a8c2490393f331f86fdeca3361b
MU3	projects/v3-periphery/contracts/Multicall3.sol	9add5c4f468ea6bdbfa899d50a2791075a5d7efb
TRSO	projects/v3-periphery/contracts/libraries/TokenRatioSortOrder.sol	84ff0b5257a032c234bf53b3866a857edd30512b
LAM	projects/v3-periphery/contracts/libraries/LiquidityAmounts.sol	90290468f2c997f1dd6ce61d5c6732ef68108353
OLI	projects/v3-periphery/contracts/libraries/OracleLibrary.sol	25b17353da9b4b350a684c055505d188ebdd7f5b
PAT	projects/v3-periphery/contracts/libraries/Path.sol	2504b1a543392240bddbe04efef9c47cecdc704b

CID	projects/v3-periphery/contracts/libraries/ChainId.sol	a2ffce157a73a5b87024ed2bb54f9c3ae19b04c3
PVA	projects/v3-periphery/contracts/libraries/PositionValue.sol	52eb32a0cd1962fbaa2729adfefaebacc2e7049a
SPMP	projects/v3-periphery/contracts/libraries/SqrtPriceMathPartial.sol	081e888ddd8d0edb80022f5baf9cfe671fdc4228
HST	projects/v3-periphery/contracts/libraries/HexStrings.sol	fc19854bf736b050ab6a78bb595cef7a43699b45
THE1	projects/v3-periphery/contracts/libraries/TransferHelper.sol	abf409eca19b2d8299659c27d32a4973addaba7d
NFTD	projects/v3-periphery/contracts/libraries/NFTDescriptor.sol	b469f8a94204d0e459beef59758f8007fb9ff98d
NFTSVG	projects/v3-periphery/contracts/libraries/NFTSVG.sol	c562b2387143eaab75fc7c01ef8b8d38d3d2da14
CVA	projects/v3-periphery/contracts/libraries/CallbackValidation.sol	3201a426afc90c023ee5e197c490fbb9f11175eb
PTC	projects/v3-periphery/contracts/libraries/PoolTicksCounter.sol	0fb778ef37f801ca66479324e3cd0f74a5f27b17
BLI	projects/v3-periphery/contracts/libraries/BytesLib.sol	747be1412bfe71b5c06f4bbfa7cb7b2c968bfdcc
PKE	projects/v3-periphery/contracts/libraries/PositionKey.sol	6cc88dd5fd105faa25c6f048b0e7da4e50263c8b
PAD	projects/v3-periphery/contracts/libraries/PoolAddress.sol	10057686fb41d92545c6262d8db8b3c228ea89c1
V3M	projects/v3-periphery/contracts/V3Migrator.sol	48caa26775c5c2392a42c6c97836ff9840a214b2

TIMV2	projects/v3-periphery/contracts/lens/TakerInterfaceMulticallV2.sol	e770de51477ab00489668ffec96ab0dfb7ce3b1b
QUO	projects/v3-periphery/contracts/lens/Quoter.sol	80ec59eac672b799172398d7d40e6e8175409322
TIM	projects/v3-periphery/contracts/lens/TakerInterfaceMulticall.sol	70549b3baa2146ab93acad834687f8ada5061405
QV2	projects/v3-periphery/contracts/lens/QuoterV2.sol	1c0767ce2bd5e483a7ac4b7f1b557a21c4cfe6da
TLE	projects/v3-periphery/contracts/lens/TickLens.sol	c02029980b042cac892e93c210d98b48f9af04ea
VTO	projects/v3-periphery/contracts/test/VToken.sol	aac72609c74f8e7def27fca6724906c3e1b3c94f
NPM	projects/v3-periphery/contracts/NonfungiblePositionManager.sol	ecfa9b31bf3a312601ebdf713e863e87bbf1f3d3
NFTDE	projects/v3-periphery/contracts/NFTDescriptorEx.sol	d35c3fcfaa5184930c0a24cc9107a637b96dcf18
SRO	projects/v3-periphery/contracts/SwapRouter.sol	6b69e3589701a06178486889edaccb592f799424
NTPD	projects/v3-periphery/contracts/NonfungibleTokenPositionDescriptor.sol	31918f976d738857337a4ac70c1afc1b7b68b9f8
NTPDOCV2	projects/v3-periphery/contracts/NonfungibleTokenPositionDescriptorOffChainV2.sol	12308981cfba7366fe06e700dcb1760bab4f7b20
LMA1	projects/v3-periphery/contracts/base/LiquidityManagement.sol	5febfb2e5cc3218dca96f75c8a27cb2b2a5b4a13
MUL	projects/v3-periphery/contracts/ba	e48264609451e31ffea549e7db3e3

	se/Multicall.sol	0815080505c
PIN	projects/v3-periphery/contracts/base/PoolInitializer.sol	ee4b2505afc70ce18e353937be33f60de4183192
BTI	projects/v3-periphery/contracts/base/BlockTimestamp.sol	e9433e812b02a43ae225b797863e5102e802ef27
PPA	projects/v3-periphery/contracts/base/PeripheryPayments.sol	ba48c46d36b30ed6efcb5809b92eb422d49f3f2d
PPWF	projects/v3-periphery/contracts/base/PeripheryPaymentsWithFee.sol	6b20212e7df6326bedc1a307111c687d6ee44e58
ERC7P	projects/v3-periphery/contracts/base/ERC721Permit.sol	402f58139a0bdc704f6b5737075454601084dc9c
PVA1	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	1faaa124f996c9f2c7fe0e01d6ec3dc1f07b51ec
CON	projects/router/contracts/libraries/Constants.sol	9f5f46b3797e661deab628727277abbd1f53f676
SRH	projects/router/contracts/libraries/SmartRouterHelper.sol	422fe4df3e1d40f7ba997dbd7e702fe95aa6d128
TVA	projects/router/contracts/lens/TokenValidator.sol	f27773691f3a3e9ee35272117afd3b98b48927c4

MRQV1	projects/router/contracts/lens/MixedRouteQuoterV1.sol	fa23af5c8521717ca8c5812a6997803acba856ca
QUO1	projects/router/contracts/lens/Quoter.sol	a48276c82210aba14d9931b639db786c0fbd98e9
QV21	projects/router/contracts/lens/QuoterV2.sol	04925f2810dfac6ed1d7336a68a5ce6af6a44efa
V3SR	projects/router/contracts/V3SwapRouter.sol	32f86ed869f3c1dee047868c2df4df8a89f08cc7
SRO1	projects/router/contracts/SmartRouter.sol	f62701207beff231fe812925fa5577ac5edb18fb
V2SR	projects/router/contracts/V2SwapRouter.sol	517222cc85024b422eae5693af30104465d56a9c
SSR	projects/router/contracts/StableSwapRouter.sol	9750ad4282333237cf8620ae3b1b4cd6b8a8f314
OSL	projects/router/contracts/base/OracleSlippage.sol	17fb66f4dcda1c4b7e374eaf93e4e83df44d5c93
AAC	projects/router/contracts/base/ApproveAndCall.sol	bd5b9e0f1a8a9216a4cab4041d27b32dc1c15bd5
PVE	projects/router/contracts/base/PeripheryValidationExtended.sol	483b82556fb058c127df7039afb4231baa8046ac
PPE	projects/router/contracts/base/PeripheryPaymentsExtended.sol	b3d877d35e3ad9dcf108a7da06f4fa5ea2ef89d4
IST	projects/router/contracts/base/ImmutableState.sol	1a8de0e5accdefb8ec7d8c289dbe8d58ad9a07dd
PPWFE	projects/router/contracts/base/PeripheryPaymentsWithFeeExtended.sol	f6bd82eb2bde6eda0b6bf12c1caf7cbf3034c41a

MEX	projects/router/contracts/base/MulticallExtended.sol	5298e2aa514b32f19f88f300845097850aa27298
SCA1	projects/masterchef-v3/contracts/libraries/SafeCast.sol	0cd843e1c910d1119af2322434690839ebf09547
MUL1	projects/masterchef-v3/contracts/utils/Multicall.sol	8137902e1c2215f98bd78d6e5a49752945133822
MCV3	projects/masterchef-v3/contracts/MasterChefV3.sol	87cd99176e0cc23608742037eb3c8039151a827b
ENU	projects/masterchef-v3/contracts/Enumerable.sol	3d4bcab22971615ffb50b69501cef461608db671
MCV3KV1	projects/masterchef-v3/contracts/keeper/MasterChefV3KeeperV1.sol	6313cf4b3c552488f9e08261ebc6af4e8097508f
MCV3KV2	projects/masterchef-v3/contracts/keeper/MasterChefV3KeeperV2.sol	1c8ac9c33672f80dbe9244ac99cd3fefd1e9069f
MCV3RV2	projects/masterchef-v3/contracts/receiver/MasterChefV3ReceiverV2.sol	cb3bb7fcf57f2ebfad13cf59c0cd071b1ab5de23
MCV3R	projects/masterchef-v3/contracts/receiver/MasterChefV3Receiver.sol	62b0d4e74e729f2072e6bd55f5932807812fe61d
SVE	projects/permit2/contracts/libraries/SignatureVerification.sol	dd68d8a975a709d84f32ae4cdd6d704c74761231
P2L	projects/permit2/contracts/libraries/Permit2Lib.sol	74762721f17b2eea2055a26cf9bac9b996565b38
SC1	projects/permit2/contracts/libraries/SafeCast160.sol	577d3a941bb6a2bf540c0c2cd6e3b6d09ca26fea
ALL	projects/permit2/contracts/libraries/Allowance.sol	65abf38fef3946cf2372fa345fdeb56769ecedc7

PHA	projects/permit2/contracts/libraries/PermitHash.sol	b2ae41e299e68016b9b033213a6abd69d6474809
ATR	projects/permit2/contracts/AllowanceTransfer.sol	4ef1cda7683e348b4ca9d033abba82c879f827bb
EIP7	projects/permit2/contracts/EIP712.sol	1df7e9ecb5d9e38872aa98f0b5e78c352ec5c8a8
STR	projects/permit2/contracts/SignatureTransfer.sol	e89404bc2e13a6a6be891fc8e67503d14de21cb3
PER	projects/permit2/contracts/PermitErrors.sol	6b971c1caf81ffc55053a962f20e9735864d1c30
PE2	projects/permit2/contracts/Permit2.sol	8d0748bd41238d9137cc39547aa0c5c249ec7001
URH	projects/universal-router/contracts/libraries/UniversalRouterHelper.sol	131b2ed283bc9a25d9706a23afef2d597c2043ad
CON1	projects/universal-router/contracts/libraries/Constants.sol	8c3cb7bfaca2cbf3361ebe1c8e32715e452cfbed
COM	projects/universal-router/contracts/libraries/Commands.sol	4266b08b499a7a26d74074d148d6c3168e383201
BLI1	projects/universal-router/contracts/libraries/BytesLib.sol	e070ff22101657beb9f7d45fa1adf130a47c6a9c
P2P	projects/universal-router/contracts/modules/Permit2Payments.sol	96d0b3a8a6b5cc2c9bd15804f23a24a9f45ae60c
PAY	projects/universal-router/contracts/modules/Payments.sol	e73f4b9f9b4ea495a1ab82b66aa43688371d4702
V3SR1	projects/universal-router/contracts/modules/takerswap/V3SwapRout	759698b7359660ff046cec12321abe03e937f5e6

	er.sol	
V2SR1	projects/universal-router/contracts/modules/takerswap/V2SwapRouter.sol	f56ef5085450603f63f4f17d0c11454daac4e07f
SSR1	projects/universal-router/contracts/modules/takerswap/StableSwapRouter.sol	0199f887274bf841bc05933c15f6eee7fd1ad9c1
SC11	projects/universal-router/contracts/permit2/src/libraries/SafeCast160.sol	f1706b39df99bc32bad76bf6cf97db904e18f329
URO	projects/universal-router/contracts/UniversalRouter.sol	a801885d1ade060532ad53d3d52c37ff55026cbb
RCO	projects/universal-router/contracts/base/RewardsCollector.sol	5fced0129cded7db27e327ec1868ed814ddab6d0
RIM	projects/universal-router/contracts/base/RouterImmutables.sol	664f69fa41662747774df15071ccc5cb21be5d6a
CAL	projects/universal-router/contracts/base/Callbacks.sol	eb44249f44806f56c080c99ede47d0432a5a3919
DIS	projects/universal-router/contracts/base/Dispatcher.sol	f7c0c1cbd20123c4faf5562d1bc30c3b8da6abb6
LAMS	projects/universal-router/contracts/base/LockAndMsgSender.sol	727309744ef36150f541200a0f0f3ce1a5163a03
LTI	projects/v3-lm-pool/contracts/libraries/LmTick.sol	c03b53848ebafc751260b470be795c510feec2f6
TV3LP	projects/v3-lm-pool/contracts/TakerV3LmPool.sol	d2260c5c62aae24165cacf525a74c0b67c665090
TV3LPD	projects/v3-lm-pool/contracts/TakerV3LmPoolDeployer.sol	3d7c72417061b48f809f5ed2f2916e30bcad752c

1.3 Issue Statistic

Item	Count	Fixed	Acknowledged
Total	1	1	0
Informational	0	0	0
Minor	1	1	0
Medium	0	0	0
Major	0	0	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 Taker Protocol to identify any potential issues and vulnerabilities in the source code of the Taker Swap 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 1 issues of varying severity, listed below.

ID	Title	Severity	Status
MCV-1	Owner Has High Authority	Minor	Fixed

3 Participant Process

Here are the relevant actors with their respective abilities within the Taker Swap Smart Contract :

User

- Users can perform swaps, add liquidity, create new trading pools, increase or decrease positions in Taker Protocol.
- Users can perform staking, withdrawal, get cumulative rewards, add or set ratios in Taker Protocol.
- `harvest` : User harvests veTaker from a pool.
- `withdraw` : User withdraws LP tokens from a pool.
- `increaseLiquidity` : User increases the liquidity of a position.
- `decreaseLiquidity` : User decreases the liquidity of a position.
- `exactInputSingle` : User swaps as much as possible of one token for another in a single transaction.
- `exactInput` : User swaps one token for another along a specified path.
- `exactOutputSingle` : User swaps a specific amount of one token for as little as possible of another in a single transaction.
- `exactOutput` : User swaps tokens along a specified path (in reverse) to achieve a specific output amount.
- `mint` : User creates a new position wrapped in an NFT.
- `burn` : User burns a token ID, deleting it from the NFT contract after liquidity and tokens are cleared.
- `flash` : User borrows token0 and/or token1 and repays them with a fee in a callback.

Admin

- Administrators can create pools and set basic parameters (such as fees, reward speed, liquidity ratio, etc).
- Administrators can modify and use privileged address permissions, emergency withdrawals, oracle updates, etc.

- `add` : Admin adds a new pool.
- `set` : Admin updates the veTaker allocation points for a given pool.
- `TakerV3Factory` : Admin deploys TakerSwap V3 pools and manages ownership and protocol fee control.
- `createPool` : Admin configures pool initialization.
- `setOwner` : Admin sets the owner of the pool.
- `enableFeeAmount` : Admin enables specific fee amounts for the pool.
- `setWhiteListAddress` : Admin sets whitelist addresses for the pool.
- `setFeeAmountExtraInfo` : Admin sets additional fee amount information.
- `setStableSwap` : Admin sets Taker Stable Swap Factory and related info.

4 Findings

MCV-1 Owner Has High Authority

Severity: Minor

Status: Fixed

Code Location:

projects/masterchef-v3/contracts/MasterChefV3.sol#245

Descriptions:

In MasterChefV3, the privileged owner account, which is not under the management of Dao, has higher permissions to modify sensitive parameters.

```
    function setReceiver(address _receiver) external onlyOwner {
        if (_receiver == address(0)) revert ZeroAddress();
        if (veTaker.allowance(_receiver, address(this)) != type(uint256).max) revert();
        receiver = _receiver;
        emit NewReceiver(_receiver);
    }

    function setLMPoolDeployer(ILMPoolDeployer _LMPoolDeployer) external onlyOwner {
        if (address(_LMPoolDeployer) == address(0)) revert ZeroAddress();
        LMPoolDeployer = _LMPoolDeployer;
        emit NewLMPoolDeployerAddress(address(_LMPoolDeployer));
    }

    function updateFarmBoostContract(address _newFarmBoostContract) external
onlyOwner {
        // farm booster can be zero address when need to remove farm booster
        FARM_BOOSTER = IFarmBooster(_newFarmBoostContract);
        emit UpdateFarmBoostContract(_newFarmBoostContract);
    }
```

Suggestion:

It is recommended to transfer privileged accounts to the intended DAO-like governance contract and change privileged operations to time-unlocked.

Resolution:

The client replied that it would use a single node in the early stage of the project to quickly build the business, and use a multi-signature wallet or Dao governance to avoid centralization risks after the project is stable.

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.