Mezo Clean Room

Mezo

HALBORN

Mezo Clean Room - Mezo

Prepared by: HALBORN

Last Updated 02/17/2025

Date of Engagement by: January 27th, 2025 - January 31st, 2025

Summary

100% OF ALL REPORTED FINDINGS HAVE BEEN ADDRESSED

ALL FINDINGS	CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
2	2	0	0	0	0

TABLE OF CONTENTS

1. Introduction

`Mezo` engaged `Halborn` to conduct a security assessment ensuring their project is not vulnerable to issues reported to a similar project without violating licensing provisions beginning on January 27th, 2025 and ending on January 31st, 2025. The security assessment was scoped to the `Mezo` project repository, further details can be found in the **Scope** section of this report.

2. Assessment Summary

The team at `Halborn` assigned one full-time security engineer to check the security of the Golang-based project. The security engineer is a Golang, blockchain, and smart-contract security expert with advanced penetration testing and smart-contract hacking skills, and deep knowledge of multiple blockchain protocols.

The purpose of this assessment is to:

- Ensure that the `Mezo` project is not vulnerable to identified potential vulnerabilities
- Where `Mezo` is vulnerable, provide guidance for remediation while maintaining clean room requirements

In summary, `Halborn` identified some issues and improvements to reduce the likelihood and impact of risks, which were fully addressed by the `Mezo team`.

3. Test Approach And Methodology

`Halborn` performed a combination of manual review of the code and automated security testing to balance efficiency, timeliness, practicality, and accuracy in regard to the scope of the smart contract assessment.

4. RISK METHODOLOGY

Every vulnerability and issue observed by Halborn is ranked based on **two sets** of **Metrics** and a **Severity Coefficient**. This system is inspired by the industry standard Common Vulnerability Scoring System.

The two **Metric sets** are: **Exploitability** and **Impact**. **Exploitability** captures the ease and technical means by which vulnerabilities can be exploited and **Impact** describes the consequences of a successful exploit.

The **Severity Coefficients** is designed to further refine the accuracy of the ranking with two factors: **Reversibility** and **Scope**. These capture the impact of the vulnerability on the environment as well as the number of users and smart contracts affected.

The final score is a value between 0-10 rounded up to 1 decimal place and 10 corresponding to the highest security risk. This provides an objective and accurate rating of the severity of security vulnerabilities in smart contracts.

The system is designed to assist in identifying and prioritizing vulnerabilities based on their level of risk to address the most critical issues in a timely manner.

4.1 EXPLOITABILITY

ATTACK ORIGIN (AO):

Captures whether the attack requires compromising a specific account.

ATTACK COST (AC):

Captures the cost of exploiting the vulnerability incurred by the attacker relative to sending a single transaction on the relevant blockchain. Includes but is not limited to financial and computational cost.

ATTACK COMPLEXITY (AX):

Describes the conditions beyond the attacker's control that must exist in order to exploit the vulnerability. Includes but is not limited to macro situation, available third-party liquidity and regulatory challenges.

METRICS:

EXPLOITABILITY METRIC (M_E)	METRIC VALUE	NUMERICAL VALUE
Attack Origin (AO)	Arbitrary (AO:A) Specific (AO:S)	1 0.2
Attack Cost (AC)	Low (AC:L) Medium (AC:M) High (AC:H)	1 0.67 0.33
Attack Complexity (AX)	Low (AX:L) Medium (AX:M) High (AX:H)	1 0.67 0.33

Exploitability E is calculated using the following formula:

$$E = \prod m_e$$

4.2 IMPACT

CONFIDENTIALITY (C):

Measures the impact to the confidentiality of the information resources managed by the contract due to a successfully exploited vulnerability. Confidentiality refers to limiting access to authorized users only.

INTEGRITY (I):

Measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and veracity of data stored and/or processed on-chain. Integrity impact directly affecting Deposit or Yield records is excluded.

AVAILABILITY (A):

Measures the impact to the availability of the impacted component resulting from a successfully exploited vulnerability. This metric refers to smart contract features and functionality, not state. Availability impact directly affecting Deposit or Yield is excluded.

DEPOSIT (D):

Measures the impact to the deposits made to the contract by either users or owners.

YIELD (Y):

Measures the impact to the yield generated by the contract for either users or owners.

METRICS:

IMPACT METRIC (M_I)	METRIC VALUE	NUMERICAL VALUE
Confidentiality (C)	None (I:N) Low (I:L) Medium (I:M) High (I:H) Critical (I:C)	0 0.25 0.5 0.75 1
Integrity (I)	None (I:N) Low (I:L) Medium (I:M) High (I:H) Critical (I:C)	0 0.25 0.5 0.75 1
Availability (A)	None (A:N) Low (A:L) Medium (A:M) High (A:H) Critical (A:C)	0 0.25 0.5 0.75 1
Deposit (D)	None (D:N) Low (D:L) Medium (D:M) High (D:H) Critical (D:C)	0 0.25 0.5 0.75 1

IMPACT METRIC (M_I)	METRIC VALUE	NUMERICAL VALUE
Yield (Y)	None (Y:N) Low (Y:L) Medium (Y:M) High (Y:H) Critical (Y:C)	0 0.25 0.5 0.75 1

Impact I is calculated using the following formula:

$$I = max(m_I) + \frac{\sum m_I - max(m_I)}{4}$$

4.3 SEVERITY COEFFICIENT

REVERSIBILITY (R):

Describes the share of the exploited vulnerability effects that can be reversed. For upgradeable contracts, assume the contract private key is available.

SCOPE (S):

Captures whether a vulnerability in one vulnerable contract impacts resources in other contracts.

METRICS:

SEVERITY COEFFICIENT (C)	COEFFICIENT VALUE	NUMERICAL VALUE
Reversibility (r)	None (R:N) Partial (R:P) Full (R:F)	1 0.5 0.25

SEVERITY COEFFICIENT (C)	COEFFICIENT VALUE	NUMERICAL VALUE
Scope (s)	Changed (S:C) Unchanged (S:U)	1.25 1

Severity Coefficient C is obtained by the following product:

$$C = rs$$

The Vulnerability Severity Score S is obtained by:

$$S = min(10, EIC * 10)$$

The score is rounded up to 1 decimal places.

SEVERITY	SCORE VALUE RANGE
Critical	9 - 10
High	7 - 8.9
Medium	4.5 - 6.9

SEVERITY	SCORE VALUE RANGE
Low	2 - 4.4
Informational	0 - 1.9

5. SCOPE

FILES AND REPOSITORY

(a) Repository: mezod

(b) Assessed Commit ID: 3884eca

(c) Items in scope:

- app\upgrades
- app\app.go
- app\app_test.go
- app\ethtest_helper.go
- app\export.go
- app\gas.go
- app\oracle.go
- app\test_helpers.go
- app\tps_counter.go
- app\tps_counter_test.go
- app\upgrades.go
- app\abci\types
- app\abci\preblock.go
- app\abci\preblock_test.go
- app\abci\proposal.go
- app\abci\proposal_test.go
- app\abci\vote_extension.go
- app\abci\vote_extension_test.go
- app\abci\types\proposal.pb.go
- app\abci\types\vote_extension.pb.go
- app\ante\ante.go
- app\ante\doc.go
- app\ante\handler_options.go
- app\ante\handler_options_test.go

- app\ante\integration_test.go
- app\ante\setup_test.go
- app\ante\sigverify.go
- app\ante\sigverify_test.go
- app\ante\utils_test.go
- app\ante\cosmos\authz.go
- app\ante\cosmos\authz_test.go
- app\ante\cosmos\eip712.go
- app\ante\cosmos\fees.go
- app\ante\cosmos\fees_test.go
- app\ante\cosmos\interfaces.go
- app\ante\cosmos\min_price.go
- app\ante\cosmos\min_price_test.go
- app\ante\cosmos\reject_msgs.go
- app\ante\cosmos\setup_test.go
- app\ante\cosmos\utils_test.go
- app\ante\evm\ante_test.go
- app\ante\evm\eth.go
- app\ante\evm\eth_test.go
- app\ante\evm\fees.go
- app\ante\evm\fees_test.go
- app\ante\evm\fee_checker.go
- app\ante\evm\fee_checker_test.go
- app\ante\evm\fee_market.go
- app\ante\evm\fee_market_test.go
- app\ante\evm\interfaces.go
- app\ante\evm\setup_ctx.go
- app\ante\evm\setup_ctx_test.go
- app\ante\evm\setup_test.go
- app\ante\evm\signverify_test.go
- app\ante\evm\sigs_test.go
- app\ante\evm\sigverify.go
- app\ante\evm\utils_test.go
- app\ante\utils\fee_checker.go

- app\ante\utils\interfaces.go
- app\ante\utils\setup_test.go
- app\upgrades\types.go
- app\upgrades\v0_3\constants.go
- app\upgrades\v0_3\forks.go
- app\upgrades\v0_3\upgrades.go
- app\upgrades\v0_4\constants.go
- app\upgrades\v0_4\forks.go
- app\upgrades\v0_5\constants.go
- app\upgrades\v0_5\forks.go
- chain\chain.go
- chain\mainnet\mezo_31612-1\genesis.json
- chain\mainnet\mezo_31612-1\seeds.txt
- chain\testnet\mezo_31611-1\genesis.json
- chain\testnet\mezo_31611-1\seeds.txt
- client\export.go
- client\import.go
- client\keys.go
- client\debug\debug.go
- client\docs\config.json
- client\docs\statik\statik.go
- client\docs\swagger-ui\favicon-16x16.png
- client\docs\swagger-ui\favicon-32x32.png
- client\docs\swagger-ui\index.html
- client\docs\swagger-ui\oauth2-redirect.html
- client\docs\swagger-ui\swagger-ui-bundle.js
- client\docs\swagger-ui\swagger-ui-standalone-preset.js
- client\docs\swagger-ui\swagger-ui.css
- client\docs\swagger-ui\swagger.yaml
- client\keys\add.go
- client\keys\utils.go
- cmd\config\config.go
- cmd\config\observability.go
- cmd\mezod\cmd_test.go

- cmd\mezod\init.go
- cmd\mezod\main.go
- cmd\mezod\root.go
- cmd\mezod\testnet.go
- cmd\mezod\genesis\account.go
- cmd\mezod\genesis\genesis.go
- cmd\mezod\genesis\migrate.go
- cmd\mezod\poa\flags.go
- cmd\mezod\poa\poa.go
- cmd\mezod\poa\submitapplication.go
- cmd\mezod\toml\get.go
- cmd\mezod\toml\set.go
- cmd\mezod\toml\toml.go
- crypto\codec\amino.go
- crypto\codec\codec.go
- crypto\ethsecp256k1\benchmark_test.go
- crypto\ethsecp256k1\ethsecp256k1.go
- crypto\ethsecp256k1\ethsecp256k1_test.go
- crypto\ethsecp256k1\keys.pb.go
- crypto\hd\algorithm.go
- crypto\hd\algorithm_test.go
- crypto\hd\benchmark_test.go
- crypto\keyring\options.go
- docs\bridge-observability.md
- docs\development.md
- docs\evm-compatibility.md
- docs\testnet.md
- docs\upgrades.md
- docs\rfc\rfc-2.md
- docs\rfc\rfc-3.md
- docs\rfc\rfc-4.md
- encoding\config.go
- encoding\config_test.go
- encoding\codec\codec.go

- ethereum\ethereum.go
- ethereum\bindings\common\gen\Makefile
- ethereum\bindings\portal\gen\gen.go
- ethereum\bindings\portal\gen\Makefile
- ethereum\bindings\portal\gen\abi\.keep
- ethereum\bindings\portal\gen\abi\BitcoinBridge.go
- ethereum\bindings\portal\gen\contract\.keep
- ethereum\bindings\portal\gen\contract\BitcoinBridge.go
- ethereum\bindings\portal\gen_address\.keep
- ethereum\bindings\portal\gen_address\BitcoinBridge
- ethereum\eip712\domain.go
- ethereum\eip712\eip712.go
- ethereum\eip712\eip712_fuzzer_test.go
- ethereum\eip712\eip712_legacy.go
- ethereum\eip712\eip712_test.go
- ethereum\eip712\encoding.go
- ethereum\eip712\encoding_legacy.go
- ethereum\eip712\message.go
- ethereum\eip712\preprocess.go
- ethereum\eip712\preprocess_test.go
- ethereum\eip712\types.go
- ethereum\sidecar\client.go
- ethereum\sidecar\client_mock.go
- ethereum\sidecar\client_test.go
- ethereum\sidecar\server.go
- ethereum\sidecar\server_test.go
- ethereum\sidecar\cli\ethereum_sidecar.go
- ethereum\sidecar\cli\flags.go
- ethereum\sidecar\types\ethereum_sidecar.pb.go
- infrastructure\cloudflare\activity\src\blockscout.ts
- infrastructure\cloudflare\activity\src\index.ts
- infrastructure\cloudflare\activity\src\progress.ts
- infrastructure\cloudflare\activity\src\types.ts
- infrastructure\cloudflare\faucet\.dev.vars.sample

- infrastructure\cloudflare\faucet\.gitignore
- infrastructure\cloudflare\faucet\deploy.sh
- infrastructure\cloudflare\faucet\package-lock.json
- infrastructure\cloudflare\faucet\package.json
- infrastructure\cloudflare\faucet\README.md
- infrastructure\cloudflare\faucet\tsconfig.json
- infrastructure\cloudflare\faucet\wrangler.toml
- infrastructure\cloudflare\faucet\src\assets.ts
- infrastructure\cloudflare\faucet\src\index.ts
- infrastructure\kubernetes\mezo-staging\helmfile.yaml
- infrastructure\kubernetes\mezo-staging\mezo-rpc.yaml
- infrastructure\kubernetes\mezo-staging\README.md
- infrastructure\kubernetes\mezo-staging\values\blockscout-stack.yaml
- infrastructure\kubernetes\mezo-staging\values\mezo-node-0.yaml
- infrastructure\kubernetes\mezo-staging\values\mezo-node-1.yaml
- infrastructure\kubernetes\mezo-staging\values\mezo-node-2.yaml
- infrastructure\kubernetes\mezo-staging\values\mezo-node-3.yaml
- infrastructure\kubernetes\mezo-staging\values\mezo-node-4.yaml
- infrastructure\kubernetes\mezo-staging\values\mezo-node-common.yaml
- infrastructure\kubernetes\mezo-staging\values\postgresql.yaml
- infrastructure\terraform\mezo-staging\.env
- infrastructure\terraform\mezo-staging\.gitignore
- infrastructure\terraform\mezo-staging\.terraform-version
- infrastructure\terraform\mezo-staging\artifact_registry.tf
- infrastructure\terraform\mezo-staging\gce.tf
- infrastructure\terraform\mezo-staging\gke.tf
- infrastructure\terraform\mezo-staging\lb.tf
- infrastructure\terraform\mezo-staging\load-secrets.sh
- infrastructure\terraform\mezo-staging\main.tf
- infrastructure\terraform\mezo-staging\nat.tf
- infrastructure\terraform\mezo-staging\oidc-github.tf
- infrastructure\terraform\mezo-staging\outputs.tf
- infrastructure\terraform\mezo-staging\providers.tf
- infrastructure\terraform\mezo-staging\README.md

- infrastructure\terraform\mezo-staging\ssl_certificates.tf
- infrastructure\terraform\mezo-staging\variables.tf
- infrastructure\terraform\mezo-staging\vpc.tf
- infrastructure\terraform\mezo-staging\remote-state\main.tf
- infrastructure\terraform\mezo-staging\ssl-certificates\mezo-staging-explorer.crt.tpl
- infrastructure\terraform\mezo-staging\ssl-certificates\mezo-staging-explorer.key.tpl
- infrastructure\terraform\mezo-staging\ssl-certificates\mezo-staging-rpc-ws.crt.tpl
- infrastructure\terraform\mezo-staging\ssl-certificates\mezo-staging-rpc-ws.key.tpl
- infrastructure\terraform\mezo-staging\ssl-certificates\mezo-staging-rpc.crt.tpl
- infrastructure\terraform\mezo-staging\ssl-certificates\mezo-staging-rpc.key.tpl
- infrastructure\terraform\mezo-staging\ssl-certificates\mezo-staging-safe.crt.tpl
- infrastructure\terraform\mezo-staging\ssl-certificates\mezo-staging-safe.key.tpl
- networks\local\Makefile
- networks\local\mezo\Dockerfile
- precompile\contract.go
- precompile\contract_test.go
- precompile\converter.go
- precompile\event.go
- precompile\event_test.go
- precompile\method.go
- precompile\method_test.go
- precompile\version_map.go
- precompile\version_map_test.go
- precompile\assetsbridge\abi.json
- precompile\assetsbridge\assets_bridge.go
- precompile\assetsbridge\assets_bridge_test.go
- precompile\assetsbridge\bridge.go
- precompile\assetsbridge\byte_code.go
- precompile\assetsbridge\IAssetsBridge.sol
- precompile\btctoken\abi.json
- precompile\btctoken\allowance.go
- precompile\btctoken\allowance_test.go
- precompile\btctoken\approve.go
- precompile\btctoken\approve_test.go

- precompile\btctoken\balance.go
- precompile\btctoken\btctoken.go
- precompile\btctoken\byte_code.go
- precompile\btctoken\IBTC.sol
- precompile\btctoken\metadata.go
- precompile\btctoken\metadata_test.go
- precompile\btctoken\permit.go
- precompile\btctoken\permit_test.go
- precompile\btctoken\setup_test.go
- precompile\btctoken\total_supply.go
- precompile\btctoken\total_supply_test.go
- precompile\btctoken\transfer.go
- precompile\btctoken\transfer_test.go
- precompile\btctoken\solidity\IERC20.sol
- precompile\btctoken\solidity\IERC20Metadata.sol
- precompile\btctoken\solidity\IERC20WithPermit.sol
- precompile\hardhat\.gitignore
- precompile\hardhat\copy-interfaces.sh
- precompile\hardhat\hardhat.config.ts
- precompile\hardhat\package-lock.json
- precompile\hardhat\package.json
- precompile\hardhat\README.md
- precompile\hardhat\tsconfig.json
- precompile\hardhat\contracts\AssetsBridgeCaller.sol
- precompile\hardhat\contracts\BTCCaller.sol
- precompile\hardhat\contracts\MaintenanceCaller.sol
- precompile\hardhat\contracts\PriceOracleCaller.sol
- precompile\hardhat\contracts\UpgradeCaller.sol
- precompile\hardhat\contracts\ValidatorPoolCaller.sol
- precompile\hardhat\scripts\accounts.ts
- precompile\hardhat\scripts\localhost-keys.ts
- precompile\hardhat\tasks\btctoken.ts
- precompile\hardhat\tasks\maintenance.ts
- precompile\hardhat\tasks\priceoracle.ts

- precompile\hardhat\tasks\upgrade.ts
- precompile\hardhat\tasks\util.ts
- precompile\hardhat\tasks\validatorpool.ts
- precompile\maintenance\abi.json
- precompile\maintenance\byte_code.go
- precompile\maintenance\evm.go
- precompile\maintenance\evm_test.go
- precompile\maintenance\IMaintenance.sol
- precompile\maintenance\maintenance.go
- precompile\maintenance\precompiles.go
- precompile\maintenance\precompiles_test.go
- precompile\maintenance\setup_test.go
- precompile\priceoracle\abi.json
- precompile\priceoracle\byte_code.go
- precompile\priceoracle\decimals.go
- precompile\priceoracle\decimals_test.go
- precompile\priceoracle\IPriceOracle.sol
- precompile\priceoracle\price_oracle.go
- precompile\priceoracle\rounds.go
- precompile\priceoracle\rounds_test.go
- precompile\priceoracle\setup_test.go
- precompile\upgrade\abi.json
- precompile\upgrade\byte_code.go
- precompile\upgrade\IUpgrade.sol
- precompile\upgrade\plan.go
- precompile\upgrade\plan_test.go
- precompile\upgrade\setup_test.go
- precompile\upgrade\upgrade.go
- precompile\validatorpool\gen
- precompile\validatorpool\abi.json
- precompile\validatorpool\application.go
- precompile\validatorpool\application_test.go
- precompile\validatorpool\byte_code.go
- precompile\validatorpool\IValidatorPool.sol

- precompile\validatorpool\owner.go
- precompile\validatorpool\owner_test.go
- precompile\validatorpool\privilege.go
- precompile\validatorpool\privilege_test.go
- precompile\validatorpool\setup_test.go
- precompile\validatorpool\validator.go
- precompile\validatorpool\validatorpool.go
- precompile\validatorpool\validator_test.go
- precompile\validatorpool\gen\validatorpool_binding.go
- proto\buf.gen.gogo.yaml
- proto\buf.gen.swagger.yaml
- proto\buf.lock
- proto\buf.yaml
- proto\ethermint\crypto\v1\ethsecp256k1\keys.proto
- proto\ethermint\evm\v1\events.proto
- proto\ethermint\evm\v1\evm.proto
- proto\ethermint\evm\v1\genesis.proto
- proto\ethermint\evm\v1\query.proto
- proto\ethermint\evm\v1\tx.proto
- proto\ethermint\feemarket\v1\events.proto
- proto\ethermint\feemarket\v1\feemarket.proto
- proto\ethermint\feemarket\v1\genesis.proto
- proto\ethermint\feemarket\v1\query.proto
- proto\ethermint\feemarket\v1\tx.proto
- proto\ethermint\types\v1\account.proto
- proto\ethermint\types\v1\dynamic_fee.proto
- proto\ethermint\types\v1\indexer.proto
- proto\ethermint\types\v1\web3.proto
- proto\mezo\abci\v1\proposal.proto
- proto\mezo\abci\v1\vote_extension.proto
- proto\mezo\bridge\v1\bridge.proto
- proto\mezo\bridge\v1\genesis.proto
- proto\mezo\bridge\v1\proposal.proto
- proto\mezo\bridge\v1\query.proto

- proto\mezo\bridge\v1\vote_extension.proto
- proto\mezo\ethereum_sidecar\v1\ethereum_sidecar.proto
- proto\mezo\poa\v1\genesis.proto
- proto\mezo\poa\v1\poa.proto
- proto\mezo\poa\v1\query.proto
- rpc\apis.go
- rpc\websockets.go
- rpc\backend\mocks
- rpc\backend\account_info.go
- rpc\backend\account_info_test.go
- rpc\backend\backend.go
- rpc\backend\backend_suite_test.go
- rpc\backend\blocks.go
- rpc\backend\blocks_test.go
- rpc\backend\call_tx.go
- rpc\backend\call_tx_test.go
- rpc\backend\chain_info.go
- rpc\backend\chain_info_test.go
- rpc\backend\client_test.go
- rpc\backend\evm_query_client_test.go
- rpc\backend\feemarket_query_client_test.go
- rpc\backend\filters.go
- rpc\backend\filters_test.go
- rpc\backend\node_info.go
- rpc\backend\node_info_test.go
- rpc\backend\sign_tx.go
- rpc\backend\sign_tx_test.go
- rpc\backend\tracing.go
- rpc\backend\tracing_test.go
- rpc\backend\tx_info.go
- rpc\backend\tx_info_test.go
- rpc\backend\utils.go
- rpc\backend\utils_test.go
- rpc\backend\mocks\client.go

- rpc\backend\mocks\evm_query_client.go
- rpc\backend\mocks\feemarket_query_client.go
- rpc\ethereum\pubsub\pubsub.go
- rpc\ethereum\pubsub\pubsub_test.go
- rpc\namespaces\ethereum\debug\api.go
- rpc\namespaces\ethereum\debug\trace.go
- rpc\namespaces\ethereum\debug\trace_fallback.go
- rpc\namespaces\ethereum\debug\utils.go
- rpc\namespaces\ethereum\eth\filters
- rpc\namespaces\ethereum\eth\api.go
- rpc\namespaces\ethereum\eth\filters\api.go
- rpc\namespaces\ethereum\eth\filters\filters.go
- rpc\namespaces\ethereum\eth\filters\filter_system.go
- rpc\namespaces\ethereum\eth\filters\subscription.go
- rpc\namespaces\ethereum\eth\filters\utils.go
- rpc\namespaces\ethereum\miner\api.go
- rpc\namespaces\ethereum\miner\unsupported.go
- rpc\namespaces\ethereum\net\api.go
- rpc\namespaces\ethereum\personal\api.go
- rpc\namespaces\ethereum\txpool\api.go
- rpc\namespaces\ethereum\web3\api.go
- rpc\types\addrlock.go
- rpc\types\block.go
- rpc\types\block_test.go
- rpc\types\events.go
- rpc\types\events_test.go
- rpc\types\query_client.go
- rpc\types\types.go
- rpc\types\utils.go
- scripts\localnet-sidecars-start.sh
- scripts\localnet-start.sh
- scripts\localnode-start.sh
- scripts\proto-tools-installer.sh
- scripts\protoc-swagger-gen.sh

- scripts\protocgen.sh
- scripts\public-testnet.sh
- server\indexer_cmd.go
- server\indexer_service.go
- server\json_rpc.go
- server\start.go
- server\util.go
- server\config\config.go
- server\config\config_test.go
- server\config\toml.go
- server\flags\flags.go
- tests\integration\ledger\ledger_test.go
- tests\integration\ledger\mezod_suite_test.go
- tests\integration\ledger\mocks\AccountRetriever.go
- tests\integration\ledger\mocks\registry.go
- tests\integration\ledger\mocks\SECP256K1.go
- tests\integration\ledger\mocks\tendermint.go
- testutil\abci.go
- testutil\ante.go
- testutil\fund.go
- testutil\setup.go
- testutil\statedb.go
- testutil\network\doc.go
- testutil\network\network.go
- testutil\network\network_test.go
- testutil\network\util.go
- testutil\tx\cosmos.go
- testutil\tx\eip712.go
- testutil\tx\eth.go
- testutil\tx\signer.go
- types\account.go
- types\account.pb.go
- types\account_test.go
- types\benchmark_test.go

- types\block.go
- types\chain_id.go
- types\chain_id_test.go
- types\codec.go
- types\coin.go
- types\dynamic_fee.go
- types\dynamic_fee.pb.go
- types\errors.go
- types\gasmeter.go
- types\hdpath.go
- types\indexer.go
- types\indexer.pb.go
- types\int.go
- types\oracle.go
- types\protocol.go
- types\validation.go
- types\validation_test.go
- types\web3.pb.go
- utils\utils.go
- utils\utils_test.go
- version\version.go
- x\bridge\module.go
- x\bridge\abci\types
- x\bridge\abci\interfaces.go
- x\bridge\abci\preblock.go
- x\bridge\abci\preblock_test.go
- x\bridge\abci\proposal.go
- x\bridge\abci\proposal_test.go
- x\bridge\abci\vote_extension.go
- x\bridge\abci\vote_extension_test.go
- x\bridge\abci\types\proposal.pb.go
- x\bridge\abci\types\vote_extension.pb.go
- x\bridge\client\cli\query.go
- x\bridge\keeper\assets_locked.go

- x\bridge\keeper\assets_locked_test.go
- x\bridge\keeper\genesis.go
- x\bridge\keeper\genesis_test.go
- x\bridge\keeper\keeper.go
- x\bridge\keeper\keeper_test.go
- x\bridge\keeper\params.go
- x\bridge\keeper\params_test.go
- x\bridge\keeper\query_server.go
- x\bridge\types\assets_locked.go
- x\bridge\types\assets_locked_test.go
- x\bridge\types\bridge.pb.go
- x\bridge\types\genesis.go
- x\bridge\types\genesis.pb.go
- x\bridge\types\genesis_test.go
- x\bridge\types\interfaces.go
- x\bridge\types\keys.go
- x\bridge\types\params.go
- x\bridge\types\query.pb.go
- x\bridge\types\query.pb.gw.go
- x\evm\genesis.go
- x\evm\genesis_test.go
- x\evm\module.go
- x\evm\client\cli\query.go
- x\evm\client\cli\tx.go
- x\evm\client\cli\utils.go
- x\evm\client\cli\utils_test.go
- x\evm\keeper\abci.go
- x\evm\keeper\abci_test.go
- x\evm\keeper\benchmark_test.go
- x\evm\keeper\block_proposer.go
- x\evm\keeper\config.go
- x\evm\keeper\fees.go
- x\evm\keeper\fees_test.go
- x\evm\keeper\gas.go

- x\evm\keeper\grpc_query.go
- x\evm\keeper\grpc_query_test.go
- x\evm\keeper\hooks.go
- x\evm\keeper\hooks_test.go
- x\evm\keeper\integration_test.go
- x\evm\keeper\keeper.go
- x\evm\keeper\keeper_test.go
- x\evm\keeper\migrations.go
- x\evm\keeper\migrations_test.go
- x\evm\keeper\msg_server.go
- x\evm\keeper\msg_server_test.go
- x\evm\keeper\params.go
- x\evm\keeper\params_benchmark_test.go
- x\evm\keeper\params_test.go
- x\evm\keeper\setup_test.go
- x\evm\keeper\statedb.go
- x\evm\keeper\statedb_benchmark_test.go
- x\evm\keeper\statedb_test.go
- x\evm\keeper\state_transition.go
- x\evm\keeper\state_transition_benchmark_test.go
- x\evm\keeper\state_transition_test.go
- x\evm\keeper\utils_test.go
- x\evm\migrations\v4\types
- x\evm\migrations\v4\migrate.go
- x\evm\migrations\v4\migrate_test.go
- x\evm\migrations\v4\types\evm.pb.go
- x\evm\migrations\v5\migrate.go
- x\evm\migrations\v5\migrate_test.go
- x\evm\migrations\v5\types\evm.pb.go
- x\evm\statedb\access_list.go
- x\evm\statedb\config.go
- x\evm\statedb\interfaces.go
- x\evm\statedb\journal.go
- x\evm\statedb\mocks.go

- x\evm\statedb\statedb.go
- x\evm\statedb\statedb_test.go
- x\evm\statedb\state_object.go
- x\evm\statedb\transient_storage.go
- x\evm\types\access_list.go
- x\evm\types\access_list_test.go
- x\evm\types\access_list_tx.go
- x\evm\types\access_list_tx_test.go
- x\evm\types\call.go
- x\evm\types\chain_config.go
- x\evm\types\chain_config_test.go
- x\evm\types\codec.go
- x\evm\types\codec_test.go
- x\evm\types\compiled_contract.go
- x\evm\types\dynamic_fee_tx.go
- x\evm\types\dynamic_fee_tx_test.go
- x\evm\types\ERC20Contract.json
- x\evm\types\errors.go
- x\evm\types\events.go
- x\evm\types\events.pb.go
- x\evm\types\evm.pb.go
- x\evm\types\genesis.go
- x\evm\types\genesis.pb.go
- x\evm\types\genesis_test.go
- x\evm\types\interfaces.go
- x\evm\types\key.go
- x\evm\types\legacy_tx.go
- x\evm\types\legacy_tx_test.go
- x\evm\types\logs.go
- x\evm\types\logs_test.go
- x\evm\types\msg.go
- x\evm\types\msg_test.go
- x\evm\types\params.go
- x\evm\types\params_legacy.go

- x\evm\types\params_test.go
- x\evm\types\precompile.go
- x\evm\types\query.go
- x\evm\types\query.pb.go
- x\evm\types\query.pb.gw.go
- x\evm\types\SimpleStorageContract.json
- x\evm\types\storage.go
- x\evm\types\storage_test.go
- x\evm\types\TestMessageCall.json
- x\evm\types\tracer.go
- x\evm\types\tx.go
- x\evm\types\tx.pb.go
- x\evm\types\tx.pb.gw.go
- x\evm\types\tx_args.go
- x\evm\types\tx_args_test.go
- x\evm\types\tx_data.go
- x\evm\types\tx_data_test.go
- x\evm\types\utils.go
- x\evm\types\utils_test.go
- x\feemarket\genesis.go
- x\feemarket\module.go
- x\feemarket\client\cli\query.go
- x\feemarket\keeper\abci.go
- x\feemarket\keeper\abci_test.go
- x\feemarket\keeper\eip1559.go
- x\feemarket\keeper\eip1559_test.go
- x\feemarket\keeper\grpc_query.go
- x\feemarket\keeper\grpc_query_test.go
- x\feemarket\keeper\integration_test.go
- x\feemarket\keeper\keeper.go
- x\feemarket\keeper\keeper_test.go
- x\feemarket\keeper\migrations.go
- x\feemarket\keeper\migrations_test.go
- x\feemarket\keeper\msg_server.go

- x\feemarket\keeper\msg_server_test.go
- x\feemarket\keeper\params.go
- x\feemarket\keeper\params_test.go
- x\feemarket\keeper\setup_test.go
- x\feemarket\keeper\utils_test.go
- x\feemarket\migrations\v4\migrate.go
- x\feemarket\migrations\v4\migrate_test.go
- x\feemarket\migrations\v4\types\feemarket.pb.go
- x\feemarket\migrations\v4\types\params.go
- x\feemarket\types\codec.go
- x\feemarket\types\errors.go
- x\feemarket\types\events.go
- x\feemarket\types\events.pb.go
- x\feemarket\types\feemarket.pb.go
- x\feemarket\types\genesis.go
- x\feemarket\types\genesis.pb.go
- x\feemarket\types\genesis_test.go
- x\feemarket\types\interfaces.go
- x\feemarket\types\keys.go
- x\feemarket\types\msg.go
- x\feemarket\types\msg_test.go
- x\feemarket\types\params.go
- x\feemarket\types\params_test.go
- x\feemarket\types\query.pb.go
- x\feemarket\types\query.pb.gw.go
- x\feemarket\types\tx.pb.go
- x\feemarket\types\tx.pb.gw.go
- x\poa\LICENSE
- x\poa\module.go
- x\poa\client\cli
- x\poa\client\cli\flags.go
- x\poa\client\cli\genval.go
- x\poa\client\cli\query.go
- x\poa\keeper\abci.go

- x\poa\keeper\abci_test.go
- x\poa\keeper\application.go
- x\poa\keeper\application_test.go
- x\poa\keeper\connect_compat.go
- x\poa\keeper\connect_compat_test.go
- x\poa\keeper\genesis.go
- x\poa\keeper\genesis_test.go
- x\poa\keeper\historical_info.go
- x\poa\keeper\historical_info_test.go
- x\poa\keeper\keeper.go
- x\poa\keeper\keeper_test.go
- x\poa\keeper\owner.go
- x\poa\keeper\owner_test.go
- x\poa\keeper\params.go
- x\poa\keeper\privilege.go
- x\poa\keeper\privilege_test.go
- x\poa\keeper\query_server.go
- x\poa\keeper\validator.go
- x\poa\keeper\validator_test.go
- x\poa\spec\01_state.md
- x\poa\spec\02_start_block.md
- x\poa\spec\03_end_block.md
- x\poa\spec\04_params.md
- x\poa\spec\README.md
- x\poa\types\application.go
- x\poa\types\errors.go
- x\poa\types\genesis.go
- x\poa\types\genesis.pb.go
- x\poa\types\historical_info.go
- x\poa\types\key.go
- x\poa\types\params.go
- x\poa\types\poa.pb.go
- x\poa\types\query.pb.go
- x\poa\types\query.pb.gw.go

- x\poa\types\validator.go

Out-of-Scope:

REMEDIATION COMMIT ID:

- https://github.com/mezo-org/mezod/tree/005d88e28928fe28d81e84dde5b32ba94cd21989

Out-of-Scope: New features/implementations after the remediation commit IDs.

6. ASSESSMENT SUMMARY & FINDINGS OVERVIEW

CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
2	0	0	0	0

SECURITY ANALYSIS	RISK LEVEL	REMEDIATION DATE
TRANSACTION EXECUTION NOT ACCOUNTING FOR ALL STATE TRANSITION AFTER INTERACTION WITH PRECOMPILES	CRITICAL	SOLVED - 02/13/2025
INCORRECT BALANCE UPDATE	CRITICAL	SOLVED - 02/13/2025

7. FINDINGS & TECH DETAILS

7.1 TRANSACTION EXECUTION NOT ACCOUNTING FOR ALL STATE TRANSITION AFTER INTERACTION WITH PRECOMPILES

// CRITICAL

Description

When processing precompiled contracts, the `StateDB` is only updated if and only if the state before and after processing differs. This leaves an attacker the ability to craft transactions which perform some actions, then mirror the initial state of the `StateDB` at completion, which will result in the intermediate actions not being committed.

BVSS

AO:A/AC:L/AX:L/R:N/S:U/C:N/A:N/I:N/D:L/Y:N (9.0)

Recommendation

The `KVStore` at `x/evm/statedb` should be modified to account for transient or intermediary changes, instead of solely relying on a differential between state A and state B to trigger a commit to the StateDB. Additionally, `Mezo` should ensure that the `KVStore` is fully synced to the EVM prior to executing a precompiled contract; if `StateDB.Commit` returns without error, this should be sufficient to ensure the states are synced.

The identified vulnerability is not currently exploitable in the `Mezo` codebase given the smart contracts currently in the repository, but could be introduced in the future due to nuanced edge cases related to the implementation of the EVM and Cosmos SDK codebases or as smart contracts are added.

Remediation

SOLVED: The **Mezo team** solved this issue.

Remediation Hash

https://github.com/mezo-org/mezod/tree/005d88e28928fe28d81e84dde5b32ba94cd21989

7.2 INCORRECT BALANCE UPDATE

// CRITICAL

Description

A discrepancy between the EVM and Cosmos state can occur due to precompiled contracts failing to explicitly update the Cosmos state DB while processing EVM transactions.

This specific issue is not currently of concern for the Mezod project but could arise in future development and iterations.

BVSS

AO:A/AC:L/AX:L/R:N/S:U/C:N/A:N/I:N/D:L/Y:N (9.0)

Recommendation

In instances where a Cosmos module is storing state information and interacting with the EVM, ensure Cosmos state is explicitly updated when EVM transactions are processed while utilizing precompiled contracts. Additionally, a record of all balance operations and the accounts they affect can be created while executing precompiled contracts to allow the reversion of actions during failure.

The identified vulnerability is not currently exploitable in the `Mezo` codebase given the smart contracts currently in the repository, but could be introduced in the future due to nuanced edge cases related to the implementation of the EVM and Cosmos SDK codebases or as smart contracts are added.

Remediation

SOLVED: The **Mezo team** solved this issue.

Remediation Hash

https://github.com/mezo-org/mezod/tree/005d88e28928fe28d81e84dde5b32ba94cd21989

Halborn strongly recommends conducting a follow-up assessment of the project either within six months or immediately following any material changes to the codebase, whichever comes first. This approach is crucial for maintaining the project's integrity and addressing potential vulnerabilities introduced by code modifications.