F Y E O

Theoriq

Repo: https://github.com/Moonsong-Labs/tq-oracle

Security Review Update: December 1, 2025

Reviewer: balthasar@gofyeo.com

Security Code Review TQ Oracle

New security issues, 3

After the development team implemented the latest updates, FYEO conducted a review of the modifications. The primary goal of this evaluation was to ensure the continued robustness of the program's security features, safeguarding user funds and maintaining the overall integrity of the program.

General Updates:

The changes in this update primarily focus on adding support for osETH (a liquid staking token) across the oracle system while addressing a price manipulation concern. The oracle previously had no way to handle osETH, which meant it either couldn't track vaults holding this asset or would be vulnerable to price manipulation through decentralized exchanges. The update introduces osETH as a recognized asset that gets priced using the protocol's own on-chain conversion mechanism rather than market prices, and ensures that other pricing adapters explicitly skip it to avoid using potentially manipulated exchange rates. This allows the system to accurately calculate total value locked while protecting against scenarios where someone could artificially depress the DEX price during the reporting window to force an artificially low valuation.

The update also includes several architectural improvements to make the asset collection system more robust and configurable. It refactors how subvault addresses are discovered by centralizing the logic into a reusable utility function that properly uses consistent blockchain state snapshots, and adds configuration options to control which assets are tracked and how expensive operations like exit queue scanning can be skipped when not needed. The changes introduce a distinction between default additional assets that should always be tracked and user-specified extras that might conflict with other specialized adapters, along with a new flag system to mark certain assets as "TVL only" so they're counted in valuations but excluded from on-chain oracle reports. Additionally, the StakeWise adapter was simplified by removing deprecated escrow-related logic and improving how it handles exit queue tickets, making the codebase cleaner and more maintainable while adding better support for scanning multiple addresses beyond just the main vault and its subvaults.

Idle Balances tvl_only Logic Inconsistency

Finding ID: FYEO-TQO-01
Severity: **Informational**
Status: **Remediated**

Description

The comment says “Only user-specified extra tokens are tvl_only” but code includes both defaults and extras in the lookup used to determine tvl_only flag.

Proof of Issue

File name: src/tq_oracle/adapters/asset_adapters/idle_balances.py
Line number: 80

```
# Only user-specified extra tokens are tvl_only to avoid conflicts with other adapters
self._additional_asset_lookup: set[str] = {
    addr.lower() for addr in self._additional_assets  # ← Includes defaults + extras
}
```

Where `self._additional_assets` contains both:

```
self._additional_assets: list[str] = [
    *self._default_additional_assets,  # Defaults included
    *self._extra_additional_assets,    # Extras included
]
```

Severity and Impact Summary

Default additional assets incorrectly marked as tvl_only, causing them to be excluded from oracle reports. Only extras should be tvl_only.

Recommendation

Make sure this behaviour is as intended. Correct documentation or create separate lookup for extras only.

StakeWise Blocking Call in Async Function

Finding ID: FYEO-TQO-02
Severity: **Informational**
Status: **Remediated**

Description

The `fetch_subvault_addresses` function is synchronous and makes blocking RPC calls, but is called directly in an async function without `asyncio.to_thread()`, blocking the event loop.

Proof of Issue

File name: src/tq_oracle/adapters/asset_adapters/stakewise.py
Line number: 226

```
async def fetch_all_assets(self) -> list[AssetData]:
    subvault_addresses = fetch_subvault_addresses(self.config)
```

Severity and Impact Summary

Blocks event loop during RPC calls, preventing other async operations from running. Defeats the purpose of async architecture.

Recommendation

Wrap in `asyncio.to_thread()`.

Test Expects Wrong Behavior for Default Additional Assets

Finding ID: FYEO-TQO-03
Severity: **Informational**
Status: **Remediated**

Description

Test `test_default_additional_tokens_not_tvl_only` has incorrect assertion. Test name says defaults should NOT be tvl_only, but assertion expects True.

Proof of Issue

File name: tests/adapters/asset_adapters/test_idle_balances.py
Line number: 157

```
def test_default_additional_tokens_not_tvl_only(config, monkeypatch):
    # ...
    report_flags = {asset.asset_address: asset.tvl_only for asset in assets}
    assert report_flags[default_token] is True  # FALSE
    assert report_flags[base_token] is False
```

Severity and Impact Summary

Default additional assets should NOT be tvl_only according to test name and comment in code, but test expects True.

Recommendation

Make sure to update the documentation to match the implementation or fix assertion to match test name.

Commit Hash Reference:

For transparency and reference, the security review was conducted on the specific commit hash for the Theoriq repository. The commit hash for the reviewed versions is as follows:

390668eac772c5a59195999dd4971e8c7d4fd59a

Remediations were submitted with the commit hash: dad346215f5f2e6fc18e6d97e3a116cb07a5f12e.

Conclusion:

In conclusion, the security aspects of the Theoriq program remain robust and unaffected by the recent updates. Users can confidently interact with the protocol, assured that their funds are well-protected. The commitment to security exhibited by the development team is commendable, and we appreciate the ongoing efforts to prioritize the safeguarding of user assets.