FYEO

Spree

Repo: https://github.com/Spree-Finance/spree-points-evm

Security Review Update: September 30, 2025

Reviewer: balthasar@gofyeo.com

Spree EVM Security Review Update

New security issues, 1

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:

This patch introduces a significant refactor aimed at streamlining the contracts and making them more general. One of the biggest changes is the renaming of the original **SpreePoints** system to simply **Points**, with the associated terminology updated across the codebase. This cleanup reduces reliance on project specific naming and makes the logic clearer and more consistent for broader use. Along with the renaming, several event signatures and function interfaces were simplified, removing unnecessary identifiers and moving toward a single-request-per-account model for redemptions rather than handling multiple concurrent requests.

In addition to the naming refactor, the contracts were updated to allow more flexibility and configurability. Instead of relying on fixed constants, key values like the token name and symbol, vault share rates, and minimum redemption thresholds are now provided at initialization or through governance controlled setters. The redemption flow has also been restructured, with clearer lifecycle management around requests, cancellations, rejections, and finalizations. Altogether, these changes modernize the design, reduce project-specific coupling, and pave the way for a more maintainable and adaptable system going forward.

Missing bound checks

Finding ID: FYEO-SPREE-01
Severity: **Low**
Status: **Remediated**

Description

The `setMinRedemRequest` function is missing a bounds check and the name has a typo. Also it is marked `public` while similar functions are `external`.
The `CollateralVault` now accepts `_assetToSharesRate` but there appears to be no bound check on this value.

Proof of Issue

File name: contracts/infra/Factory.sol
Line number: 253

```
function setMinRedemRequest(uint256 min) public {
    _checkRole(EXECUTOR_ROLE);
    minRedemRequest = min;
}
```

File name: contracts/infra/CollateralVault.sol
Line number: 60

```
function __CollateralVault_init(address asset_, address _factory, uint256
_assetToSharesRate) internal onlyInitializing {
    ...

    assetToSharesRate = _assetToSharesRate;
}
```

Severity and Impact Summary

Mistakes in configuration could lead to division by zero errors.

Recommendation

Make sure to establish upper and lower bounds for all configuration values to avoid potential mistakes.

Commit Hash Reference:

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

1c395b2899e300197208d0db9ae60cde9a2b2032

Remediations have been submitted with the commit hash
7eab11621175d8aeb8da506ffca7a0c5c21238ef.

Conclusion:

In conclusion, the security aspects of the Spree 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.