FYEO

Spree

Security Review Update: August 11, 2025

Reviewer: balthasar@gofyeo.com

Spree 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:

The codebase has undergone extensive refactoring, with a focus on centralizing configuration logic, enhancing access control mechanisms, and introducing new account structures. Key changes include the introduction of functions for updating redemption executors, authorities, and freeze states, all of which require strict authorization checks. Centralized `Config` accounts now manage fee parameters, freezing status, and authority roles, replacing legacy structures such as `Fees` and `FreezeState`. These changes aim to improve modularity, security, and auditability but introduce critical security implications, particularly around access control enforcement, constraint validation, and event logging.

Specific Security Changes:

Decimals mismatch on init: `args.decimals` can differ from `SP_DECIMALS` while `SP_PER_USDC` and math assume 6 decimals - enforce/validate decimals or store/use decimals in conversion logic.

InitTokenAccountArgs.decimals is allowed to vary but contract assumes SP_DECIMALS = 6

Finding ID: FYEO-SPREE-01
Severity: Medium
Status: Remediated

Description

The token initialization accepts `args.decimals` and uses it for `mint::decimals = args.decimals`. However the program constants and arithmetic assume SP has 6 decimals (`SP_DECIMALS: u8 = 6`) and a fixed conversion `SP_PER_USDC = 100`. If an initializer supplies a different `decimals`, conversion math (e.g. `usdc_amount = amount / SP_PER_USDC`) and other logic will be incorrect, possibly undercharging/overcharging or causing loss of funds/rounding errors.

Proof of Issue

File name: programs/spree_points/src/instructions/initialize_token.rs
Line number: 79

```
#[account(
    init,
    payer = signer,
    seeds = [TOKEN_2022_SEED],
    bump,
    mint::decimals = args.decimals,
    mint::authority = mint_authority,
    mint::token_program = token_program2022,
    extensions::metadata_pointer::authority = signer,
    extensions::metadata_pointer::metadata_address = mint,
    extensions::transfer_hook::authority = signer,
    extensions::transfer_hook::program_id = args.transfer_hook_program_id,
)]
pub mint: Box<InterfaceAccount<'info, Mint2022>>,
```

File name: programs/transfer-hook/src/constants.rs
Line number: 18

```
#[constant]
pub const SP_DECIMALS: u8 = 6;

#[constant]
pub const USDC_DECIMALS: u8 = 6;

// USDC - 6 decimals | SP - 6 decimals
#[constant]
pub const SP_PER_USDC: u64 = 100;
```

Severity and Impact Summary

If a different `decimals` is used at mint creation, all token accounting that assumes 6 decimals (conversion to/from USDC, fees, `SP_PER_USDC` scaling, integer division) will be incorrect. Consequences include incorrect USD charging, rounding losses, inflation/deflation of balances, and potential financial loss or economic exploitation.

Recommendation

Enforce fixed decimals: Remove `decimals` from `InitTokenAccountArgs` and set `mint::decimals = SP_DECIMALS` in the accounts macro. This makes decimals an invariant of the program.

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: e65347205f2f560bdad9d7f3c7274d1de69a9483

Remediations were made with the commit hash: 3fc6474e95dc0593a528ec3ec1dbb759d0b77360

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.