Superform Superrewards
Security Review

Cantina Managed review by:
Defsec, Security Researcher
High Byte, Security Researcher

April 23, 2024

Contents

1 Introduction **2**
- 1.1 About Cantina . . . 2
- 1.2 Disclaimer . . . 2
- 1.3 Risk assessment . . . 2
  - 1.3.1 Severity Classification . . . 2

2 Security Review Summary **3**

3 Findings **4**
- 3.1 Low risk . . . 4
  - 3.1.1 Violation of Effect-Interaction Pattern in `_forge` Function . . . 4
  - 3.1.2 Inaccurate availableToMint Tracking During Forge Operations . . . 4
- 3.2 Informational . . . 5
  - 3.2.1 Usage of `MAX_MINT` in minting operations . . . 5
  - 3.2.2 Lack of two-step ownership transfer . . . 5

1 Introduction

1.1 About Cantina

Cantina is a security services marketplace that connects top security researchers and solutions with clients. Learn more at cantina.xyz

1.2 Disclaimer

Cantina Managed provides a detailed evaluation of the security posture of the code at a particular moment based on the information available at the time of the review. While Cantina Managed endeavors to identify and disclose all potential security issues, it cannot guarantee that every vulnerability will be detected or that the code will be entirely secure against all possible attacks. The assessment is conducted based on the specific commit and version of the code provided. Any subsequent modifications to the code may introduce new vulnerabilities that were absent during the initial review. Therefore, any changes made to the code require a new security review to ensure that the code remains secure. Please be advised that the Cantina Managed security review is not a replacement for continuous security measures such as penetration testing, vulnerability scanning, and regular code reviews.

1.3 Risk assessment

Severity	Description
Critical	*Must* fix as soon as possible (if already deployed).
High	Leads to a loss of a significant portion (>10%) of assets in the protocol, or significant harm to a majority of users.
Medium	Global losses <10% or losses to only a subset of users, but still unacceptable.
Low	Losses will be annoying but bearable. Applies to things like griefing attacks that can be easily repaired or even gas inefficiencies.
Gas Optimization	Suggestions around gas saving practices.
Informational	Suggestions around best practices or readability.

1.3.1 Severity Classification

The severity of security issues found during the security review is categorized based on the above table. Critical findings have a high likelihood of being exploited and must be addressed immediately. High findings are almost certain to occur, easy to perform, or not easy but highly incentivized thus must be fixed as soon as possible.

Medium findings are conditionally possible or incentivized but are still relatively likely to occur and should be addressed. Low findings a rare combination of circumstances to exploit, or offer little to no incentive to exploit but are recommended to be addressed.

Lastly, some findings might represent objective improvements that should be addressed but do not impact the project's overall security (Gas and Informational findings).

2 Security Review Summary

Superform is a non-custodial yield marketplace. It allows other DeFi protocols to permissionlessly list yield opportunities and users to then access them from any EVM chain.

On Mar 25th the Cantina team conducted a review of superrewards-contracts on commit hash 8f4278ac. The team identified a total of **4** issues in the following risk categories:

- Critical Risk: 0
- High Risk: 0
- Medium Risk: 0
- Low Risk: 2
- Gas Optimizations: 0
- Informational: 2

3 Findings

3.1 Low risk

3.1.1 Violation of Effect-Interaction Pattern in `_forge` Function

Severity: Low risk

Context: SuperFrens.sol#L277-L277

Description: The `_forge` function in the `SuperFrens` contract violates the Effect-Interaction pattern, which is a best practice in Solidity development. The Effect-Interaction pattern dictates that state changes (effects) should be performed before external interactions to prevent re-entrancy attack.

Violating the Effect-Interaction pattern can potentially lead to re-entrancy attack. If the _burn or _mint functions are re-entered during their execution, the state variables (`editionTiersSupply`) may be updated incorrectly, leading to inconsistencies in the contract's data.

Additionally, the `_mint` function can potentially call the `onERC1155Received` function on the receiver contract if the receiver is a contract address.

Recommendation: To follow the Effect-Interaction pattern correctly and mitigate potential security vulnerabilities, including those related to the `onERC1155Received` function, the _forge function should be modified as follows:

```
/// @notice helper function for processing forge
function _forge(uint256 tierId_) internal {
    // ...

    /// @dev adjust the edition tier supply
    /// NOTE: edition id starts from zero
    unchecked {
        console.logUint((tierId_ / TOTAL_TIERS_PER_EDITION));
        console.logUint((forgeId / TOTAL_TIERS_PER_EDITION));

        editionTiersSupply[(tierId_ / TOTAL_TIERS_PER_EDITION)][tierId_].currentSupply -= FORGE_QTY;
        editionTiersSupply[(forgeId / TOTAL_TIERS_PER_EDITION)][forgeId].currentSupply += MAX_MINT;
    }

    /// @dev burn 5 of this tierId and mint 1 above
    _burn(msg.sender, tierId_, FORGE_QTY);
    _mint(msg.sender, forgeId, MAX_MINT, ZERO_BYTES);

    // ...
}
```

Superform: Fixed in commit 98e6f4d5.

Cantina Managed: Fix is verified.

3.1.2 Inaccurate availableToMint Tracking During Forge Operations

Severity: Low risk

Context: SuperFrens.sol#L262-L262

Description: The `SuperFrens` contract contains a logical inconsistency in the management of the `availableToMint` variable during the forging process. Specifically, when a user forges new tokens by burning a specific quantity of lower-tier tokens to mint a higher-tier token, the contract adjusts the `currentSupply` for both involved tiers correctly. However, it fails to adjust the `availableToMint` for the higher tier being minted. This omission can lead to inaccurate tracking of the total number of tokens that are available for minting.

Recommendation: To rectify this oversight, it's recommended to modify the `_forge` function to include logic that decrements the `availableToMint` count for the tier of tokens being burned and increments the `availableToMint` count for the tier being minted. This adjustment ensures that `availableToMint` accurately reflects the total supply of each tier after a forge operation.

Superform: Acknowledged. The `forge` feature is not linked to the `availableToMint` variable. The `availableToMint` variable tracks the Merkle leaves that have been claimed and are yet to be claimed.

Cantina Managed: Acknowledged. `supplyClaimedByWallet` is not adjusted on the forge also. Than it's intended.

Superform: Yes, forge is not the same as claim. So it should be intended.

3.2 Informational

3.2.1 Usage of `MAX_MINT` in minting operations

Severity: Informational

Context: SuperFrens.sol#L255-L255

Description: The `SuperFrens` contract inconsistently uses the `MAX_MINT` constant and literal values (e.g., "1") in minting operations. Specifically, in the `_mintTokens` function, NFTs are minted one at a `_mint(to_, i, 1, ZERO_BYTES);`, regardless of the defined `MAX_MINT` value.

Recommendation: To ensure consistency and maintainability of the code, it's recommended to use the `MAX_MINT` constant uniformly across all minting operations.

Superform: Fixed in 98e6f4d5.

Cantina Managed: Fix is verified.

3.2.2 Lack of two-step ownership transfer

Severity: Informational

Context: SuperFrens.sol#L15-L15

Description: To change the owner address, the current contract owner can call the `Ownable.transferOwnership()` function and set a new address and this new address assumes the role immediately.

If the new address is inactive or not willing to act in the role, there is no way to restore access to that role. Therefore, the owner role can be lost.

Recommendation: It is recommended to use the following Ownable2Step library instead of Ownable library.

Superform: Acknowledged.

Cantina Managed: Acknowledged.