Fixed Point Solutions, LLC

Points Tokenization Assessment

2024/07/13
Prepared by: Kurt Barry

1. Scope

The Rumpel Wallet extends the popular Gnosis Safe multisig wallet for use with the Rumpel Protocol, which tokenizes points, allowing them to be used financially on-chain prior to their redeemability for “reward” tokens. It limits user actions and provides a hook for the Rumpel protocol to take certain actions necessary for claiming rewards for which tokenized points may be redeemed. Users place a high degree of trust in Rumpel admins/governance, but there are mechanisms to reduce this trust (allowing certain actions to always be performed, and permanently disallowing admins/governance from performing certain actions).

Commit 521f2b24 of the rumpel-wallet repository and Gnosis Safe code at tag v1.3.0 were reviewed with 12 hours of effort. All files under the src/ directory of rumpel-wallet were considered in-scope, and Gnosis Safe code was reviewed on an as-needed basis to assess integration correctness.

2. Limitations

No assessment can guarantee the absolute safety or security of a software-based system. Further, a system can become unsafe or insecure over time as it and/or its environment evolves. This assessment aimed to discover as many issues and make as many suggestions for improvement as possible within the specified timeframe. Undiscovered issues, even serious ones, may remain. Issues may also exist in components and dependencies not included in the assessment scope.

3. Findings

Findings and recommendations are listed in this section, grouped into broad categories. It is up to the team behind the code to ultimately decide whether the items listed here qualify as issues that need to be fixed, and whether any suggested changes are worth adopting. When a response from the team regarding a finding is available, it is provided.

Findings are given a severity rating based on their likelihood of causing harm in practice and the potential magnitude of their negative impact. Severity is only a rough guideline as to the risk an issue presents, and all issues should be carefully evaluated.

Severity Level Determination		Impact		
		High	Medium	Low
Likelihood	High	**Critical**	**High**	**Medium**
	Medium	**High**	**Medium**	**Low**
	Low	**Medium**	**Low**	**Low**

Issues that do not present any quantifiable risk (as is common for issues in the Code Quality category) are given a severity of **Informational**.

Summary of Findings	
Severity	Count
Critical	0
High	0
Medium	1
Low	0
Informational	1

3.1 Safety and Correctness

Findings that could lead to harmful outcomes or violate the intentions of the system.

SC.1 Users and Protocols Can Collude to Steal Rewards Because RumpleGuard Allows DELEGATECALL

Severity: Medium

Code Location: https://github.com/sense-finance/rumpel-wallet/blob/521f2b24040a463a04c63a064d83f3b8d2adad38/src/RumpelGuard.sol#L33

Description: When an (address, function selector) pair is enabled via the RumpleGuard, it becomes possible for Rumpel wallets to either CALL or DELEGATECALL that pair. Whenever the address is an upgradeable contract, this could be exploited by upgrading it so that the allowed function now overwrites the guard address; wallet owners can then eliminate the guard from wallet, allowing them to call any function. In particular, they could remove the RumpelModule, preventing the Rumpel protocol from claiming rewards that are intended for PToken redemption.

Concretely, an attack could evolve as follows:

1. A function on an upgradable contract is allowed by the RumpelGuard; the entity that controls this contract notices and creates a Rumpel wallet to start farming PTokens.
2. PTokens are sold as they are collected by the entity.
3. Very near to when rewards become claimable based on the farmed points, the entity upgrades the contract to allow overwriting the RumpelGuard address via DELEGATECALL. The entity (and any other participating wallets) clears the guard address and removes the Rumpel module. The upgradeable contract can be reverted to its original logic once this is done.
4. The entity (and other participating Rumpel users) can now claim reward tokens for itself, rugging PToken holders.

Although this may be rather unlikely if the protocols being used for point farming are trustworthy, the high severity still makes it a concerning threat vector.

Recommendation: Only allow CALL operations to (address, selector) tuples via the RumpelGuard to eliminate the possibility of this attack. Alternatively, if DELEGATECALL is deemed necessary to allow in some cases, extend the logic to enable explicitly whitelisting CALL or DELEGATECALL on a granular basis.

Response:

FPS:

3.2 Usability and Incentives

Findings that could lead to suboptimal user experience, hinder integrations, or lead to undesirable behavioral outcomes.

No significant usability or incentive issues were identified.

3.3 Gas Optimizations

Findings that could reduce the gas costs of interacting with the protocol, potentially on an amortized or averaged basis.

No significant gas optimizations were found, and minor efficiency improvements were not a focus of this assessment.

3.4 Code Quality

CQ.1 Typos

Severity: **Informational**

Code Location:
[1]https://github.com/sense-finance/rumpel-wallet/blob/521f2b24040a463a04c63a064d83f3b8d2adad38/src/RumpelGuard.sol#L62

Description:
[1]: “guarntees” should be “guarantees”
[2]: “and admin” should be “an admin”

Recommendation: Correct typos to improve readability.

Response:

FPS: