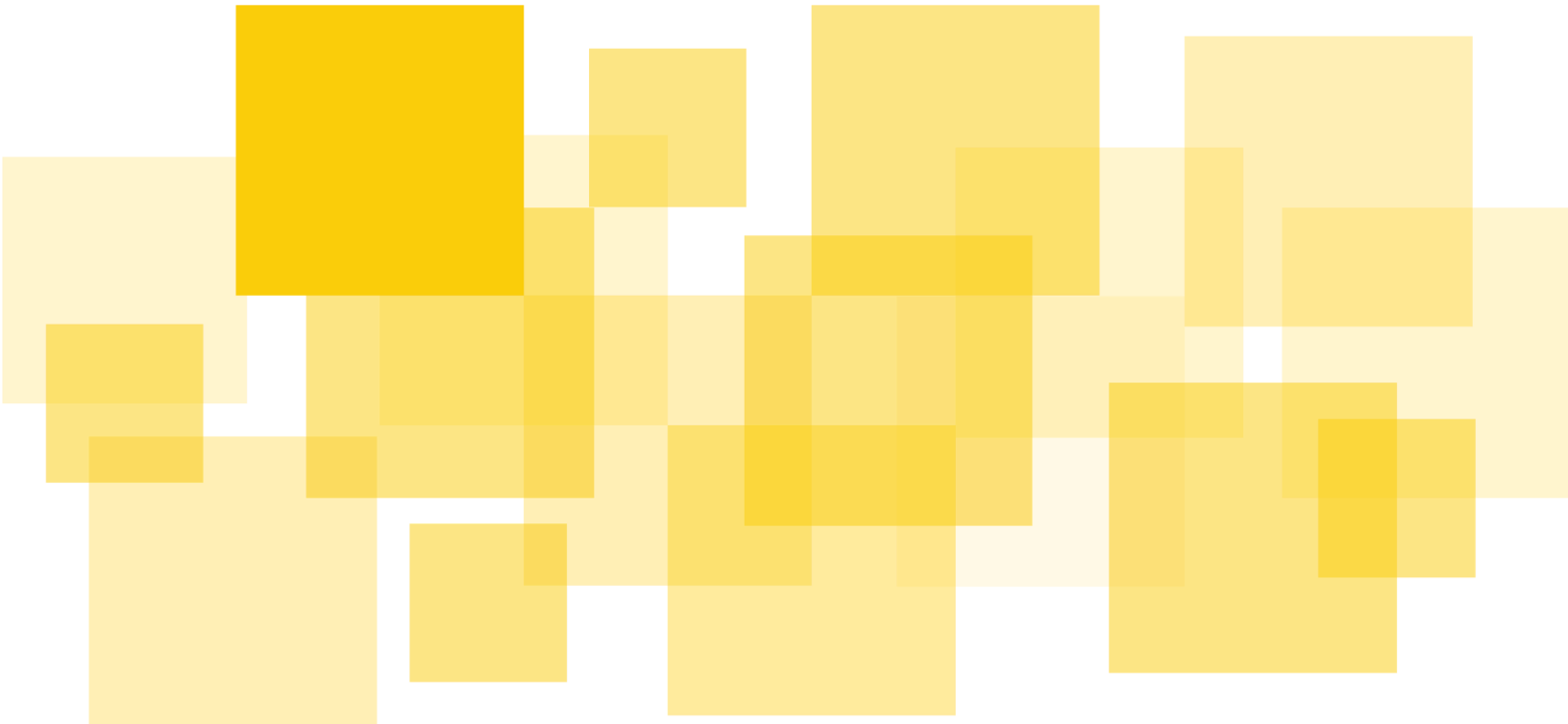
Security Audit Findings Summary

Soroswap Aggregator

Delivered: August 31st, 2024



Prepared for PaltaLabs by

runtime verification

The following table summarizes the audit findings, as well as their severity and difficulty to execute:

Finding	Severity	Difficulty	Status
[A1] Adapters Can Be Hijacked By Third-Parties: if timed right, a malicious user that monitors the admin or the deployer of Adapters can initialize newly created Adapters and point them to custom, unknown, third-party controlled contracts.	**Medium**	**Medium**	**Addressed**
[A2] Malformed Paths on Swap Requests Are Allowed by the Aggregator: when requesting swaps, the absence of checks on the addresses of assets informed in each swap path may result in unpredictable behavior and possible loss to the user/caller.	**Low**	**Low**	**Partially Addressed**
[A3] Subcontracts called from Aggregator have the potential to call into malicious code: the ability for underlying contracts to upgrade implies that there is always a chance that a protocol the Aggregator accesses could be upgraded to malicious code, which may lead users to execute it.	**High**	**High**	**Addressed**

Below is a summary of the informational findings:

Finding	Status
[B1] Best Practices and Notable Particularities: notes on the protocol particularities, comments, and suggestions to improve the code or the business logic of the protocol in a best-practice sense.	**Partially Addressed**
[B2] Administrative Functions Have Redundant Validations: the Aggregator's administrative functions have redundant checks based on data created at initialization time.	**Addressed**
[B3] Redundant Validations in the Aggregator and Underlying Contracts: the aggregator performs checks over the parameters provided by the users, which are performed once more within the underlying contracts.	**Addressed**
[B4] The Aggregator May Try to Trade Negligible Amounts: if a user attempts to trade a negligible amount of assets, the Aggregator allows it, potentially incurring the loss of assets to the user due to precision loss.	**Addressed**
[B5] The Aggregator Stores Dynamically Sized Data in Instance Storage: the aggregator stores dynamic data in instance storage, which is limited and may cause denial of services for certain of its functionalities.	**Not Addressed**

All findings have a severity level and an execution difficulty level, ranging from low to high, as well as categories in which it fits. For more information about the classifications of the findings, refer to our Smart Contract Analysis page (adaptations performed where applicable).