G0 Group

# Security Review of

## Argent Wallet

March 2021

# Argent / March 2021

## Files in scope

https://github.com/argentlabs/argent-contracts/tree/c33ff5906efcdbedfea649200e6451f00d295a9d

All solidity files in the above repository, except those contained in this folder:
`contracts/infrastructure/dapp`

## Current status

All found issues have been fixed or addressed.

# Report

## Issues

### 1. Missing return statements

***Severity: minor***

`TransactionManager.multiCallWithGuardians`, `TransactionManager.multiCallWithGuardiansAndStartSession` and `TransactionManager.multiCallWithSession` are missing return statements.

***status - fixed***

The issue is no longer present in

https://github.com/argentlabs/argent-contracts/tree/f055092bad9ca8590aa974e17d30d59b6a0df4de

### 2. Refund signature in WalletFactory can be replayed

***Severity: medium***

Refund signature in `WalletFactory` doesn't contain wallet address, so if one owner has multiple wallets, it can be replayed.

***status - fixed***

The issue is no longer present in

https://github.com/argentlabs/argent-contracts/tree/f055092bad9ca8590aa974e17d30d59b6a0df4de

### 3. It's possible to bypass transfer limitation in paused state by whitelisting a refund address

***Severity: major***

An attacker that gains control of the owner address can call `TransactionManager.addToWhitelist` before the wallet is locked by guardians and then execute a relayed transaction with a large gasPrice to the newly whitelisted address calling one of the functions that can be called in paused state, for example `TransactionManager.enableERC1155TokenReceiver`.

***status - fixed***

The issue is no longer present in

https://github.com/argentlabs/argent-contracts/tree/f055092bad9ca8590aa974e17d30d59b6a0df4de

## 4. TransactionManager.recoverSpender parsing spender incorrectly in some cases

***Severity: medium***

`TransactionManager.recoverSpender`, the function can't tell difference between `ERC20 transferFrom` and `ERC721 transferFrom` and in case of `ERC20` it will incorrectly identify `sender` as `spender`, the same thing can happen even in case of `ERC721 transferFrom` calls when the wallet is approved to transfer by a different address. There's a similar issue with `ERC1155 safeTransferFrom` calls in the situation when the wallet is an operator for a different address.

***status - fixed***

The issue is no longer present in

https://github.com/argentlabs/argent-contracts/tree/f055092bad9ca8590aa974e17d30d59b6a0df4de

## 5. DappRegistry.confirmFilterUpdate can restore recently removed Dapp

***Severity: medium***

`DappRegistry.confirmFilterUpdate` can restore recently removed Dapp if there's a pending filter update when the dapp is removed.

***status - fixed***

The issue is no longer present in

https://github.com/argentlabs/argent-contracts/tree/f055092bad9ca8590aa974e17d30d59b6a0df4de

## 6. Owner can be added as guardian despite restrictions that attempt to prevent it

***Severity: minor***

The invariant enforced in `SecurityManager` that owner can't be guardian can be broken if guardian addition is initiated before recovery for the same address is confirmed, or if recovery is initiated before guardian addition is confirmed.

***status - acknowledged***