G₀ Group

Security Review of
Argent Factory & ENS update

March 4, 2020

Argent Factory and ENS update / February 2020

Files in scope

Following solidity files present in the repository at this commit

https://github.com/argentlabs/argent-contracts/tree/ff1a5097de697c56becc23d766e33ea9dc92241c

```
contracts/
    ens/
        ArgentENSManager.sol
        ArgentENSResolver.sol
        ENSResolver.sol
        ENSReverseRegistrar.sol
        IENSManager.sol
    wallet/
        WalletFactory.sol
        BaseWallet.sol
    storage/
        GuardianStorage.sol
```

Current status

As of March 4th 2020 all raised issues have been fixed by the developer.

Issues

1. Guardian address should be part of salt for create2 call when deploying new wallets

Type: security / Severity: medium

In `WalletFactory.createCounterfactualWalletWithGuardian`, `_guardian` should be part of the salt, otherwise there's no deterministic relationship between wallet address and management rights.

status - fixed

Issue has been fixed and is no longer present in:https://github.com/argentlabs/argent-contracts/tree/945a01ad3ad0fd8bfa94dff4bfe3f44c765fd64a

Notes

2. Redundant code in WalletFactory

Type: code quality / Severity: minor

`createCounterfactualWallet` seems to be redundant copy of `createCounterfactualWalletWithGuardian`, same with createWallet and `createWalletWithGuardian`, potential gas savings don't seem worth the doubling of code.

status - fixed

Issue has been fixed in:https://github.com/argentlabs/argent-contracts/tree/945a01ad3ad0fd8bfa94dff4bfe3f44c765fd64a

3. Wallet owner has full control over the reverse ENS record of the wallet.

Type: informational

It should be kept in mind that wallet owner can at any time change resolver, owner and ttl of the reverse ENS node.

4. It should be kept in mind that wallet owner can at any time change resolver, owner and ttl of the reverse ENS node.

Type: informational

There doesn't seem to be an explicit need right now, when`claimWithResolver` call is invoked in `WalletFactory`, to transfer the ownership of the reverse ENS node to the`ArgentENSManager`, if it is to allow change of resolver for the node in the future, #1 means that it might not be possible in all cases.