G₀ Group

Security Review of
Authereum

June 17, 2020

Authereum / June 2020

Files in scope

All solidity files in the following folders present in the repository at this commit

https://github.com/authereum/authereum-contracts-audit/tree/bacd547aa851091aa4e5a4cea4f746009d52136a

```
contracts/
    account/
    modules/
    upgradeability/
    validation/
```

Current status

As of June 16th all raised issues have been fixed by the developer

Issues

1. Metatransaction submitter can force an expensive transaction to fail by not providing enough gas while still collecting reward and burning nonce

Type: security / Severity: medium

In case of very expensive meta transactions, it is possible to force this call:`(bool success, bytes memory res) = address(this).call(_encodedTransactions);` in `BaseMetaTxAccount._atomicExecuteMultipleMetaTransactions` to run out of gas, while still retaining enough gas to finish the parent transaction thanks to EIP 150. This allows submitters to collect reward without properly executing metatransactions.

status - fixed

Issue has been fixed and is no longer present in
https://github.com/authereum/contracts/commit/4a778540362efe6cec4d501ff5ed36c5327131fb

2. Ownership of contracts deployed through create2 factory is not deterministically tied to the address, limiting usage

Type: usability / Severity: medium

In `AuthereumProxyFactory.createProxy`, `_initData` should probably be part of salt so future owner can trust the address before deployment.

status - fixed

Issue has been fixed and is no longer present in
https://github.com/authereum/contracts/commit/4a778540362efe6cec4d501ff5ed36c5327131fb

3. Redundant usage of re-entrancy guard in DelegateKeyModule.executeTransaction

Type: optimisation / Severity: minor

Re-entrancy guard on `DelegateKeyModule.executeTransaction` is not necessary and should be removed to avoid inflating gas cost by unnecessary storage writes.

status - fixed

Issue has been fixed and is no longer present in
https://github.com/authereum/contracts/commit/4a778540362efe6cec4d501ff5ed36c5327131fb