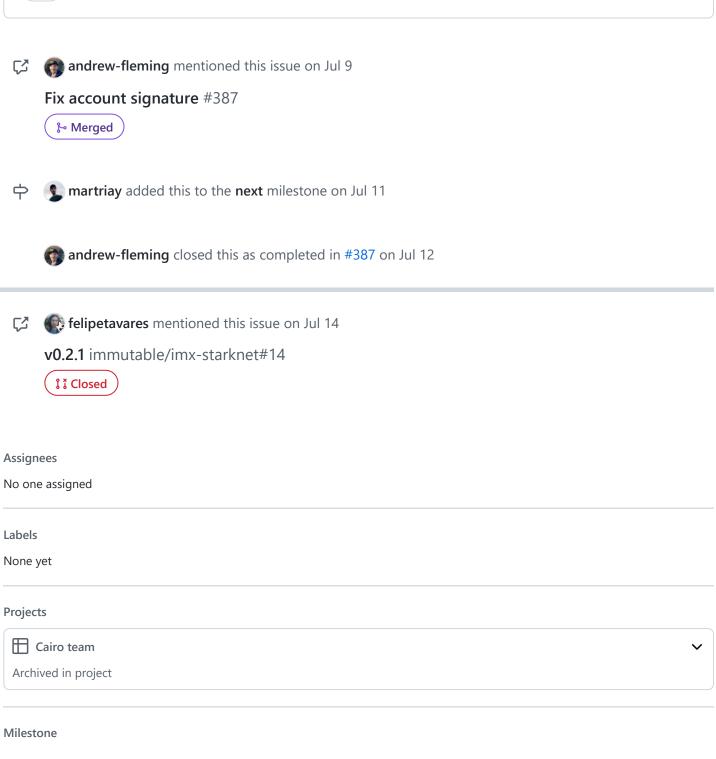
☐ OpenZeppelin / cairo-contracts (Public) <> Code • Issues 45 ! Pull requests 7 • Discussions Actions U Security 1 · · · Jump to bottom New issue ecdsa_ptr points to reference in Account lib's execute #386 andrew-fleming opened this issue on Jul 9 · 0 comments · Fixed by #387 ✓ Closed Milestone andrew-fleming commented on Jul 9 • edited • Collaborator Transactions on goerli fail with the following error message: 🛑 The transaction was rejected but no contract address was identified in the error message. Error message: Error at pc=0:133: Got an exception while executing a hint. Cairo traceback (most recent call last): Unknown location (pc=0:746) Unknown location (pc=0:682) Error message: Account: invalid signature Unknown location (pc=0:347) Unknown location (pc=0:321) Traceback (most recent call last): File "<hint14>", line 1, in <module> File "/app/src/starkware/starknet/services/batcher/starknet batcher venvsite/starkware/cairo/lang/builtins/signature/signature_builtin_runner.py", line 94, in add_signature), f"Signature hint must point to the signature builtin segment, not {addr}." AssertionError: Signature hint must point to the signature builtin segment, not 14:0. Neither the StarkNet test environment nor the devnet raise this error. The error stems from here: https://github.com/OpenZeppelin/cairo-contracts/blob/release-0.2.0/src/openzeppelin/account/library.cairo#L203 let (local ecdsa_ptr : SignatureBuiltin*) = alloc()

The Signature hint points to this reference (which the SignatureBuiltinRunner does not like). To resolve this, I suggest adding the ecdsa_ptr: SignatureBuiltin* as an implicit arg to execute, eth_execute, and _unsafe_execute in the Account library and EthAccount's __execute__ as well.

Another solution would be to isolate the functionality of both accounts (thus removing _unsafe_execute), so we don't have to pass the implicit ecdsa_ptr in the EthAccount methods.



current



Development

Successfully merging a pull request may close this issue.

> Fix account signature

andrew-fleming/cairo-contracts

2 participants



