Missing Protection against Signature Replay Attacks

Description

It is sometimes necessary to perform signature verification in smart contracts to achieve better usability or to save gas cost. A secure implementation needs to protect against Signature Replay Attacks by for example keeping track of all processed message hashes and only allowing new message hashes to be processed. A malicious user could attack a contract without such a control and get message hash that was sent by another user processed multiple times.

Remediation

In order to protect against signature replay attacks consider the following recommendations:

- Store every message hash that has been processed by the smart contract. When new messages are received check against the already existing ones and only proceed with the business logic if it's a new message hash.
- Include the address of the contract that processes the message. This ensures that the message can only be used in a single contract.
- Under no circumstances generate the message hash including the signature. The ecrecover function is susceptible to signature malleability (see also SWC-117).