Zodiac EIP-712 and EIP-1271 Signature Authentication / October 2023

Files in scope

All solidity files in
https://github.com/gnosis/zodiac/tree/b899e962e79d8d62b74df5fa6ed4570faee99bae/contracts:

Current status

All discovered issues have been fixed or addressed. No known issues are present in:
https://github.com/gnosis/zodiac/tree/3d56dc2ab34dd699f4b9d43108a20e5a0568db63/contracts

Issues

1. Nonce series shared between signatures from different agents

type: usability / severity: minor

In `SignatureChecker` the same nonce series is shared across all modules. This is potentially problematic since it requires coordination between different agents and also allows griefing by malicious consumption of nonces used in signatures of other modules.

status - fixed

The issue has been fixed and is no longer present in:
https://github.com/gnosis/zodiac/tree/3d56dc2ab34dd699f4b9d43108a20e5a0568db63/contracts

2. msg.sender instead of the module address passed to Guard.checkTransaction in GuardableModifier

type: incorrect implementation / severity: major

In `GuardableModifier.exec` and `GuardableModifier.execAndReturnData` instead of passing the address of the module that initiated the transaction to `Guard.checkTransaction`, `msg.sender` or the address of the transaction executor is passed. This prevents the Guard from properly validating the module address.

status - fixed

The issue has been fixed and is no longer present in:
https://github.com/gnosis/zodiac/tree/3d56dc2ab34dd699f4b9d43108a20e5a0568db63/contracts

3. in SignatureChecker salt is accidentally appended to the signature in the isValidSignature call

type: incorrect implementation / severity: medium

Due to incorrect slicing of msg.data, salt is appended to the signature when IERC1271.isValidSignature call is made.

status - fixed

The issue has been fixed and is no longer present in:
https://github.com/gnosis/zodiac/tree/3d56dc2ab34dd699f4b9d43108a20e5a0568db63/contracts