G0 Group

Security Review of

Zodiac Roles Modifier v2

April 2023

Zodiac Roles Modifier v2 / April 2023

Files in scope

All solidity files in https://github.com/gnosis/zodiac-modifier-roles/tree/5d218a4b6b6d01412abac07a2a7582d07dd35a65/packages/evm/contracts:

Current status

All discovered issues have been fixed or addressed. No known issues are present in:
https://github.com/gnosis/zodiac-modifier-roles/tree/c824d7b2b71f3dece080686640e51754bc57a654/packages/evm/contracts

Issues

1. Allowance conditions should be decidable at the moment other conditions are being evaluated, otherwise operators like OR might not work as expected

type: incorrect implementation / severity: medium

Currently, the amount of spent allowances is tracked in the process of evaluating conditions and compared against allowance balance only after the call has been made. In the process of evaluating conditions all allowance conditions are temporarily considered passing before the check has been made. This means that in case of an OR condition for example, if there's a combination of allowance check and other condition and the allowance check fails, it's no longer possible to go back and find out if the other condition and the whole OR is passing or not. To fix this, the code should be revised to check the allowance condtions at the same time other conditions are being checked.

status - fixed

The issue has been fixed and is no longer present in:https://github.com/gnosis/zodiac-modifier-roles/tree/c824d7b2b71f3dece080686640e51754bc57a654/packages/evm/contracts

2. In PermissionBuilder.setAllowance it should be ensured that maxBalance is >= balance

type: inconsistency / severity: medium

In `PermissionBuilder._accruedAllowance` if `maxBalance <= balance`, the balance will be capped if `timestamp >= allowance.refillTimestamp` but not otherwise, to prevent this inconsistency it should be ensured in `PermissionBuilder.setAllowance` `maxBalance` is always `>= balance`.

status - fixed

The issue has been fixed and is no longer present in:https://github.com/gnosis/zodiac-modifier-roles/tree/c824d7b2b71f3dece080686640e51754bc57a654/packages/evm/contracts

3. The implicit limit on number of conditions of 65536 should be explicitly enforced

type: security / severity: medium

Due to the way the number of conditions is packed into the header in`BufferPacker.packHeader` there's an upper limit of `65536` on the number of conditions before the value overflows, this limit should be explicitly enforced in the `Integrity` contract.

status - fixed

The issue has been fixed and is no longer present in:https://github.com/gnosis/zodiac-modifier-roles/tree/c824d7b2b71f3dece080686640e51754bc57a654/packages/evm/contracts

4. It should be ensured that first condition node is also the root node and that no other condition node is a root node

type: inconsistency / severity: minor

In `Integrity` it should be ensured that the first node in the list is also a root node, meaning it has itself as a parent and that there are no other root nodes in the list.

status - fixed

The issue has been fixed and is no longer present in:https://github.com/gnosis/zodiac-modifier-roles/tree/c824d7b2b71f3dece080686640e51754bc57a654/packages/evm/contracts

5. Implicit assumption in PermissionChecker._arraySubset that condition arraySubset nodes won't have more than 256 children should be enforced

type: security / severity: medium

In `PermissionChecker._arraySubset` due to the size of`taken` variable, the amount of child nodes of the `arraySubset` condition has to be limited to`256`, this should be enforced in the `Integrity` contract.

status - fixed

The issue has been fixed and is no longer present in:https://github.com/gnosis/zodiac-modifier-roles/tree/c824d7b2b71f3dece080686640e51754bc57a654/packages/evm/contracts