Smart Contract Audit Report

Contract Name: StorageVictim	Version: 0.4.23
Audit Performed By: Marcellus Ifeanyi	Date: 07/11/2023
No. of contracts: 1	No. of Functions: 3

Table of Contents

Findings

Vulnerability: CRITICAL

i. Uninitialized Pointer Vulnerability:

The Storage pointer `str` is uninitialized. Due to this `str.user` points to address `0` by default which is the contract owner's address.

Audit-Fix / Recommended Change:

Initialize the str to `Storage memory str;` in the store and getStore functions

POC:

- Buggy: `store(){}`

```
function store(uint _amount)  public  {
   Storage str;
    str.user =  msg.sender;
    str.amount = _amount;
    storages[msg.sender]  = str; }
```

- Audited/Fixed: `store(){}`

```
function store(uint256 amount) public {
       Storage memory str;

       str.user = msg.sender;

       str.amount = amount;

       storages[msg.sender] = str;
   }
```

- Buggy: `getStore(){}`

```
function getStore() public view returns (address, uint) {
    Storage str = storages[msg.sender];

    return (str.user, str.amount);
   }
```

- Audited/Fixed: `getStore(){}`

```
 function getStore() public view returns (address, uint256) {

       Storage storage str = storages[msg.sender];

       return (str.user, str.amount);
   }
```

Vulnerability: MEDIUM

ii. Outdated solidity compiler:

The contract uses an outdated version of solidity which might introduce certain vulnerabilities and would not be compatible with recent versions of solidity compiler

Audit Fix / Recommended Change:

Change the solidity compiler version to a more recent version.

POC:

```
  pragma  solidity ^0.4.23;
```

```
pragma solidity ^0.8.18;
```

Vulnerability: INFORMATIONAL

iii. Missing SPDX-License-Identifier

There is no definition of a license identifier, which might flag as an error in certain development environment.

Audit Fix / Recommended Change:

Add a specified License identifier, you could use `unlicensed` or a specific identifier.

Vulnerability: INFORMATIONAL

iv. Address owner can be marked `immutable`:

Since the address of the owner is designed to be assigned only once at construction, deployment gas could be saved by marking the owner address variable as `immutable`.

Audit Fix / Recommended Change:

State variable `owner` should be marked as immutable.

POC:

```
  address owner;
```

```
   address immutable owner;
```

Summary

The contract `StorageVictim` contains 1 critical vulnerability, 1 medium vulnerability and 2 informational vulnerability. The recommended update might be helpful in enhancing the security of the contract.

The `StorageSecured` contract contains the fix and audited code based on the findings

Disclaimer

This audit report might not contain all the bugs. So it is advised to perform further testing before deploying the contract to production.