

Unprotected Ether Withdrawal

Description

Due to missing or insufficient access controls, malicious parties can withdraw some or all Ether from the contract account.

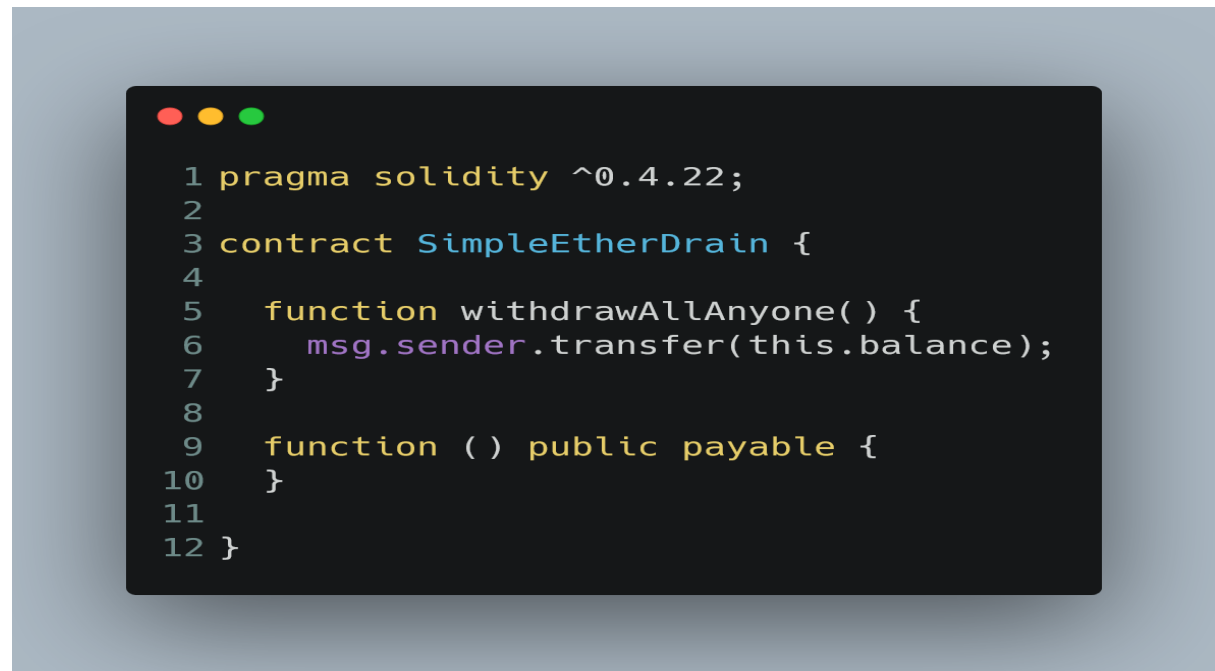
This bug is sometimes caused by unintentionally exposing initialization functions. By wrongly naming a function intended to be a constructor, the constructor code ends up in the runtime byte code and can be called by anyone to re-initialize the contract.

Remediation

Implement controls so withdrawals can only be triggered by authorized parties or according to the specs of the smart contract system.

Example:

Code:



```
1 pragma solidity ^0.4.22;
2
3 contract SimpleEtherDrain {
4
5     function withdrawAllAnyone() {
6         msg.sender.transfer(this.balance);
7     }
8
9     function ( ) public payable {
10    }
11
12 }
```

Explanation:

The "WithdrawAllAnyone" function may be used by any contract user, allowing anyone to take the entire balance.

The contract owner must implement the access control mechanism to prevent this misconfiguration.