Web3 Security Researcher:

Yahaya BabsAudits
Solidity Contract Auditor | Blockchain Devel...

Withdraw bug: Reverts when withdrawing the full balance; should use if(payment[msg.sender] < value) revert(...).
Using .transfer is unsafe for contracts due to the 2300 gas limit.

✕ BUG

Vault.sol

```
function withdraw(uint value) external {
        // ✕ BUG-1
        if (payment[msg.sender] <= value) revert("insufficient balance");
        .
        .
        payable(msg.sender).transfer(value);
}

function collectFee() external onlyOwner {
        // ✕ BUG-2
        payable(msg.sender).transfer(address(this).balance);
}
```

✓ FIX

Vault.sol

```
function withdraw(uint value) external nonReentrant {
        // ✓ FIX-1
        if (value > payment[msg.sender]) revert insufficientBalance();
```

```
        .
        .
        emit withdrawn(value, collect, msg.sender);
    }

    function collectFee() external onlyOwner {
        // ✓ FIX-2
        (bool success, ) = payable(msg.sender).call{value: amount}("");
        if (!success) revert TransferFailed();
        emit feeCollected(amount, msg.sender);
    }
```

FIX: Selected key fixes from several important suggestions