BUSDWallet

Findings and Analysis Report

31st July, 2023

Table Of Contents

Overview

An audit carried out on a BUSDWallet contract on the 31st of July, 2023. This audit spanned a period of one and a half hours.

Auditor

Anthony, (0xfps)

Summary

Slither was used in this audit as a static analyzer, and it made 3 findings, and the auditor made 5 findings. The findings are grouped into 1 critical, 2 lows, 5 informationals.

Scope

The audit covered the BUSDWallet.sol contract and its IBEP20.sol interface.

Findings

Critical

1. Funds are transferred from contract balance, not from caller balance

```
ftrace | funcSig
function sendToken(address to↑, uint256 amount↑) external {
    require(to↑ != address(0), "Invalid Address");
    require(amount↑ <= balanceToken(msg.sender), "Insufficent Fund");

    // @audit Transfers from contract balance.
    busdToken.transfer(to↑, amount↑);
    emit Transfer(to↑, msg.sender, amount↑);
}
```

The sendToken's busdToken.transfer() (BUSDWallet#18) function sends BUSD tokens from the contract to whatever address passed as `to` and it is open to be called by anyone.

An attacker can take a loan of 1 BUSD and drain the contract of all BUSD it has and repay the loan.

Remedy
Use the transferFrom() and send from `msg.sender` to `to`.

Low

1. Wrong implementation of generic Transfer event.
The universal TransferEvent on contracts are Transfer(from, to, amount) (BUSDWallet#9), however this contracts implements a Transfer(to, from, amount) which might lead to errors for event listeners.

Remedy
Switch to Transfer(from, to, amount).

2. No checks for zero address in the constructor.
There are no checks for setting the busdToken to a zero address and no method to change the address value, leading to the contract being rendered useless.

Informational

1. Import of the entire interface.
Instead of doing an `import "./IBEP20.sol";`, do an `import {IBEP20} from "./IBEP20.sol";`.

2. Pragma version 0.8.20 (BUSDWallet.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.8.18.

3. BUSDWallet.busdToken (BUSDWallet.sol#7) should be immutable

4. BUSDWallet.sendToken(address,uint256) (BUSDWallet.sol#14-20) ignores return value by busdToken.transfer(to,amount)

Conclusion

The audit took a period of 30 to 45 minutes, and it was a solo audit.