SECBOOK

「智能合约安全审计报告」

合约名称：EON

合约名称：EON

合约地址：0x4CB10F4df4BF4F64D4797d00D468181EF731Be9A

开始日期：2019.06.26

完成日期：2019.06.26

审计类型及结果：

该合约源于以太坊 ERC20 数字货币标准，用于发布代币，具备基本的代币转移、授权等功能，未见复杂业务逻辑，故审计重点集中于代码规范。

序号	审计类型	审计子项	审计结果
1	代码规范审计	ERC20 规范性	通过
		构造与析构函数规范性	通过
		函数异常处理	通过
		应急响应能力	通过
2	函数调用审计	Call 调用	通过
		Delegatecall 调用	通过
		外部合约调用	通过
3	整型溢出审计	—	通过
4	权限控制审计	—	通过
5	重入攻击审计	—	通过
6	交易顺序依赖审计	—	通过
7	时间戳依赖审计	—	通过
8	假充值审计	—	通过

详 情

代码规范审计

- **ERC20 规范性审计：**

暂未发现异常。

- **函数异常处理：**

```
function _transfer(address _from, address _to, uint _value) internal {
        … …
        uint previousBalances = balanceOf[_from] + balanceOf[_to];
        balanceOf[_from] -= _value;
        balanceOf[_to] += _value;
        Transfer(_from, _to, _value);
        assert(balanceOf[_from] + balanceOf[_to] == previousBalances);
}
```

该合约于 _transfer 处使用
assert(balanceOf[_from] + balanceOf[_to] == previousBalances);
检测 Transfer 前后双方 balance 总值，当出现异常时跳出。经测试该代码功能正常生效，能够成功中断交易。

- **应急响应能力：**

一个完备的合约除了能正确的处理请求外，还需保证在发生意外时能立即采取应对方式，及时止损，该合约未见冻结业务相关功能，尚需完善。

- **构造与析构函数规范性：**

暂未发现异常。

【综述】该代码基本符合规范，经审计暂未发现安全风险。

函数调用审计

- **Call 调用：**

未发现 Call 调用

- **Delegatecall 调用：**

非发现 Delegatecall 调用

- **外部合约调用：**
  暂未发现异常。

整型溢出审计

该合约于 balance 处理前皆存在 require 校验请求参数，未发现整型溢出可能。

```
function TokenERC20(
        uint256 initialSupply,
        string tokenName,
        string tokenSymbol
) public {
        totalSupply = initialSupply * 10 ** uint256(decimals);
        balanceOf[msg.sender] = totalSupply;
        name = tokenName;
        symbol = tokenSymbol;
}
```

于构造函数处的 totalSupply 参数虽存在上溢可能性，但其本身只于合约创建时由所有者调用，故不会引发相应威胁。

权限控制审计

该合约不存在敏感函数，权限控制得当，暂未发现威胁。

重入攻击审计

该合约使用 transfer 处理交易，暂未发现重入可能性。

交易顺序依赖审计

该合约未见复杂逻辑，条理清晰，暂未发现交易顺序依赖漏洞。

时间戳依赖审计

该合约未见时间戳相关应用逻辑，暂未发现时间戳依赖漏洞。

假充值审计

暂未发现假充值漏洞。

官网：x.secbook.io

邮箱：info@secbook.io