

[下载pdf](#)

[下载word](#)

# 智能合约安全检测报告 (以太坊)

## 基本信息

报告编号:

**781150805666299904**

报告时间:

**2020年11月25日 00:41**

项目名称:

**Prometheum**

合约文件名:

**ESV.sol**

合约hash:

**9cf81b195234bb19f277b3116ffbcce6**

- 1 -

## 检测结果

- 2 -

[下载pdf](#)
[下载word](#)

1	模糊分析	Timestamp Dependency/时间戳依赖	✓
		Exception Disorder/未抛出异常	✓
		Gasless Send/send调用gas不足	✓
		Integer Overflow/上溢	✓
		Integer Underflow/下溢	✓
		Freezing Ether/以太坊黑洞	✓
		Tx.origin Dependency/权限依赖检测	✓

序号	检测方法	检测项	检测结果
----	------	-----	------

[下载pdf](#)
[下载word](#)

		ReasonString/异常消息	✓
		State Visibility/状态变量可见性	!
		Unused Vars/未使用的变量	✓
		Visibility Modifier Order/修饰器顺序	!
		RTLO/非法字符	✓
		Shadowing State/状态变量覆盖	✓
		Shadowing Abstract/继承状态覆盖	✓

序号	检测方法	检测项	检测结果
2	静态分析	Uninitialized Storage/未初始化指针	✓
		Uninitialized State/未初始化变量	✓

下载pdf      下载word

执行异常数量: 6

说明：模糊测试可以在evm上动态的执行合约，生成边缘测试用例发现隐藏较深的漏洞，目前默认每个合约执行120秒，如有需要可联系相关人员对您的合约进行更长时间的深度模糊测试。

合约漏洞汇总

总合约数: 1

合约名称	漏洞	行号
ESV	State Visibility	6 8 9 11 12 14 15 17 18 20 22

[下载pdf](#)[下载word](#)

一站式智能合约安全测试平台

### 建议


#### State Visibility

Variables in the smart contract can be specified as public, internal or private, and the visibility of all state variables needs to be explicitly defined.

#### Visibility Modifier Order

Visibility modifier must be first in list of modifiers

[下载pdf](#)    [下载word](#)

 一站式智能合约安全测试平台

## 免责声明

本次检测仅针对ContractGuard产品涵盖检测类型及结果表中给 定的检测类型范围进行审计，其他未知安全漏洞不在本次审计责任范围之内。深信科创仅根据本报告出具前已经存在或发

下载pdf      下载word

2018-11-24 14:44:44



一站式智能合约安全测试平台

官方网址

<https://www.guardstrike.com/#/>

电子邮箱

[contact@guardstrike.com](mailto:contact@guardstrike.com)

[下载pdf](#)    [下载word](#)

