北京链安
Chains Guard Technology

智能合约安全评级接口

说明和调用

目录

一 产品介绍

以太坊平台现在共有数百万个智能合约，并且一直保持着稳定的日增长率，同时以太坊合约采用的 Solidity 语言也被诸多公链兼容。对于这些合约的安全性问题、代码规范问题，现在的审计方法以人工审计为主。

为提升智能合约开发效率，以及提升合约常见安全问题、代码规范检查的效率，北京链安基于特征代码匹配和形式化验证技术的优点，开发了 solidity 智能合约安全检测系统，凭借该系统，可以对基于 solidity 开发的合约进行合约安全扫描和快速的漏洞检测。

同时，我们将该能力通过 API 的方式开放出来，区块链生态中的任何参与者都可以通过调用该 API 对合约代码进行安全性和规范性的检测，并得到详细的反馈结果。

二 适用范围

基于 solidity 语言或者兼容 solidity 语言开发智能合约的公链的相关智能合约，如以太坊合约。

三 接口调用

1.1 传递合约地址扫描（Get）

```
curl -X GET \
 'http://$ip:$port/eth/contract/scan/address?address=$contract_addr'
```

$ip:$port 为北京链安服务提供的正式地址变量，本文档版本对应参数为：tokenrating.chainsguard.com:7000

1.2 传递合约内容扫描（Post）

```
curl -X POST \
http:// $ip: $port /eth/contract/scan/code \
-H ’content-type: multipart/form-data; \
-F code=”contract_source_code”
```

注意只有传递合约地址进行扫描的时候才能给出安全评级。

如扫描 BNB 的合约地址，请求评级结果，构造 get 请求，请求如下地址。

http://tokenrating.chainsguard.com:7000/eth/contract/scan/address?address=0xB8c77482e45F1F44dE1745F52C74426C631bDD52

主要返回字段

```
"token_name": "BNB ",
"contract_name": "BNB",
"description": "Binance aims to build a world-class crypto exchange, powering the future of crypto finance.",
"score": "92",
"grade": "AA",
```

1.3 传递 showall 参数返回所有合约评级（Get）

```
curl -X GET   \
’http://$ip: $port/eth/contract/showall’
```

四 合约扫描返回评级信息

目前评级等级包括十个等级：

AAA、AA、A、BBB、BB、B、CCC、CC、C、F

安全评级由上往下逐步降低，一般 A 以上为较为安全的或经过了市场长期检验的相对安

全的合约；BBB 至 B 等级安全程度也基本可靠；CCC 到 F 等级安全风险较高。

五 合约扫描返回细节信息

3.1 细节信息介绍

1) info

info 提示在合约中检测到的需要开发者注意的关键信息，主要给开发人员进行二次人工确认。

2)warning

warning 表示合约中的代码命中匹配规则，认为可能诱发安全漏洞。

3.2 细节信息详细描述

3.2.1 info 信息的详细条目

1)未授权写入问题

检测到 owner 的变量的赋值，给出提示。

问题等级: info

问题类型: unauthorized assignment

问题描述: Contract owner or creater ,transferOwnership function possible found. Contract fields that can be modified by any user must be inspected. Please review this function is not vulnerable.

2)伪随机数安全检测

伪随机数生成使用了可以预测的参数，给出提示。

问题等级: info

问题类型: bad random number

问题描述: Some block info or variable is found. please confirm PRNG(pseudo-random number generator) is safe.

3)tx.origin 不正确的使用

问题等级: info

问题类型: misuse of tx.origin

问题描述: Authorization checks based on the tx.origin can result in dangerous callback attacks. Please review this function is not vulnerable.

4)编译器版本不确定

编译器版本不确定，以太坊早期编译器版本存在 bug，可能导致构造函数安全问题或者产生某些漏洞。

问题等级: info

问题类型: uncertain compiler version

问题描述: Solidity compiler version is not found.

5)检测到构造函数进行信息提示

问题等级: info

问题类型: constructor detected

问题描述: Constructor function is found. Please review constructor function is not vulnerable.

6)检测到循环语句

问题等级: info

问题类型: loop function detected.

问题描述: Please review the count of loop cannot be controled .

7)检测到退款函数

问题等级: info

问题类型: refund funtion detected

问题描述: Refund is found, Please confirm balances[msg.sender] is setted to 0.

8)assembly 关键字检测

问题等级: info

问题类型: assembly keyword detected

问题描述: Assembly keyword is found. The use of assembly should be minimal. A developer should not allow a user to assign arbitrary values to function type variables.

3.2.2 warning 信息的详细条目

1)未授权写入问题

问题等级: warning

问题类型: unauthorized assignment

问题描述: Please confirm that the function assigns the owner member is private or internal . Unrestricted writing indicate parts in the contract storage that are universally writable by all users. This can be extremely dangerous if the writing are to sensitive fields of the contract, such as owner.

2)不安全的 call 和 delegatecall 提示

问题等级: warning

问题类型: unsafe call or delegatecall

问题描述: Unsafe using delegatecall or call potentially lead to inject data issue.

3)不安全的析构函数

问题等级: warning

问题类型: unsafe selfdestruct or suicide function

问题描述: The operation destruct contract unrestricted.

4)call.value()导致的重入错误提示

问题等级: warning

问题类型: reentry attack risks

问题描述: Unsafe call.value calling potentially lead to re-entrancy vulnerability.

5)整数溢出代码提示

问题等级: warning

问题类型: integer overflow

问题描述: The operation might cause integer overflow.

6)tx.origin 不正确的使用

问题等级: warning

问题类型: authorization through tx.origin

问题描述: Tx.origin should not be used for authorization.

7) 过时的 erc20 标准问题

出现了 deprecated 中的关键字，需要使用 solidity 最新开发规则中推荐使用的最新的关键字。

Deprecated	Alternative

Deprecated	Alternative
suicide(address)	selfdestruct(address)
block.blockhash(uint)	blockhash(uint)
sha3(...)	keccak256(...)
callcode(...)	delegatecall(...)
Throw	revert()
msg.gas	gasleft
Constant	view

问题等级: warning

问题类型: use of deprecated solidity functions

问题描述: Use of deprecated solidity functions.

8)编译器版本安全问题

版本声明时应该固定于某一个固定的版本或者特定版本

问题等级: warning

问题类型: unknown compiler version

问题描述: Please using pragma lock solidity compiler to specific version.

9)构造函数书写问题会被编译成正常的函数

0.4.22 版本之前的构造函数名称应该是合约名字。

0.4.22 版本之后的合约构造函数声明应使用 constructor

问题等级: warning

问题类型: unsafe constructor function

问题描述: Constructor might be compiled to a normal function,leading a possible vulnerability.

10)transfer 或者 approve 函数应该返回一个 bool 类型的值

问题等级: warning

问题类型: incompatible erc20 standard

问题描述: The function contains transfer or approve should return bool.

11)transfer 或者 approve 函数应该触发一个事件

问题等级: warning

问题类型: incompatible erc20 standard

问题描述: The function contains transfer or approve should emit event.

12)transfer 函数应该检测转账条件是否符合，并且检测转账地址不为空

问题等级: warning

问题类型: unsafe transfer funtion

问题描述: Transfer function should use require keywords throw a exception making return value is zero and making sure to address is not zero.

13)对 allowance 检测防止提前交易

问题等级: warning

问题类型: race condition issuse

问题描述: Approve have exist race condition. Maybe forget write require((_amount ==

0)||(allowed[msg.sender][_spender] == 0).

14)检测到 assert 建议替换为 require

问题等级: info

问题类型: incompatible erc20 standard

问题描述: Please replace assert keyword by require keyword in judgment statement.

15)检测到 send 建议换成 transfer

问题等级: warning

问题类型: incompatible erc20 standard

问题描述: Please replace send function by transfer function.

16)检测到成员变量没有赋予权限将被自动划分为 public 变量

问题等级: warning

问题类型: state variable default visibility

问题描述: Variables can be specified as being public, internal or private. Explicitly define visibility for all state variables.

17)结构体声明需要注明 storage 或者 memory

问题等级: warning

问题类型: access of uninitialized pointer

问题描述: It is recommended to explicitly specify the data location memory or storage when dealing with complex types to ensure they behave as expected.

18)函数忘记声明权限

问题等级: warning

问题类型:function default visibility

问题描述: Functions that do not have a function visibility type specified are public by default. This can lead to a vulnerability if a developer forgot to set the visibility and a malicious user is able to make unauthorized or unintended state changes.

六 返回字段示例和解释

4.1 返回字段示例


```
{
    data": {
        "sha256": "31a56a0a53566b3dce303c4d8706d4a5b8fa703e1097385fb29d01c967bf00ab",
        "balance_usd": 142.89,
        "contract_addr": "0x08d32b0da63e2C3bcF8019c9c5d849d7a9d791e6",
        "contract_source_code": "",
        "token_name": "BNB (BNB)",
        "dateVerified": null,
        "code": "",
        "token_rating": 167088,
        "token_link": "",
        "is_top_token": true,
        "compiler_version": "v0.4.8+commit.60cc1668",
        "scan_warning_count": 4,
        "token": "",
        "description": "",
        "short_token": "",
        "contract_name": "BNB",
        "holdings_count": 18,
        "token_transfers": "F",
        "balance_eth": "5.520433765 Ether",
        "updated": "2019-01-29 01:43:28",
        "standard": "ERC-20",
        "scan": [
            {
                "sha256": "",
                "cve": "",
                "severity": "warning",
                "name": "",
```

```
                "type": "unknown compiler version",
                "address": "",
                "func": "",
                "timestamp": "",
                "updated": "",
                "scan_version": null,
                "code": "",
                "comment": "",
                "lines": "1",
                "description": "Please using pragma lock solidity compiler to specific
version."
            } ],
        "token_addr": "0x08d32b0da63e2C3bcF8019c9c5d849d7a9d791e6",
        "transactions": "639,145 txns ",
        "scan_information_count": 19,
"grade": "AA",
"score": "92",
"open_source": "true",
        "creator_address": "0x00c5e04176d95a286fcce0e68c683ca0bfec8454"
    },
    "status_code": 10200,
    "msg": "sucess"
}
```


4.2 返回字段解释

json	返回 json	status_code	状态码 10200/10404		
		msg	返回消息：“success/not found”		
		data	数据部	compiler_version	编译器版本
				token_transfers	保留
				transactions	交易数
				token_addr	保留
				code	合约源码
				scan	扫描结果是一个 list
				holdings_count	持有代币数量
				updated	保留
				contract_name	合约名称
				token_name	关联通证
				token_rating	保留

				standard	保留
				contract_addr	合约地址
				dateVerified	保留
				balance_eth	以太币余额
				sha256	保留
				creator_address	合约创建者地址
				is_top_token	保留
				balance_usd	保留
				scan_information_count	information 的数量
				scan_warning_count	warning 的数量
				token	关联通证
				short_token	关联通证缩写
				description	合约描述
				token_link	合约链接
				open_source ("true"/"false")	是否开源
				grade（例如”AA”）	安全等级
				score("0"-"100")	得分

scan 中每个元素	扫描结果列表的元素	name	漏洞名称
		severity	严重性
		lines	行号
		scan_version	扫描版本
		updated	保留
		sha256	保留
		comment	保留
		address	保留
		code	漏洞代码
		timestamp	保留
		type	保留
		cve	保留
		description	漏洞描述
		func	保留

七 关于北京链安

北京链安网络科技有限公司，聚焦区块链生态安全，提供包括不限于交易所、钱包、主链 和矿池的安全服务，并向区块链在政务、金融、征信、物联网、商品溯源等领域的行业应

用提供全面的安全解决方案，旨在为区块链生态提供全面的安全能力。

北京链安团队具备完善的公链漏洞挖掘和项目代码审计能力，可提供全面的链上数据监测和项目代码审计服务以及链安评测和链安评级服务，曾经协助 EOS、以太坊等知名公链官方发现并修复漏洞。更有行业领先的 C 端安全能力，在 APP 代码防破解能力、本地存储数据安全、漏洞检测、开发及审计等 C 端底层技术安全方面均具有成熟的安全方案。

官方网站：https://www.chainsguard.com/
联系邮箱：biz@chainsguard.com