Fido 审 计 报 告

Version 1.0.1

报告编号：2021051400031019

灵踪安全发布

2021年5月14日

灵踪安全
FAIRYPROOF

01. 介绍

本报告包含了灵踪安全在Fido团队要求下对Fido项目的合约源代码进行审计的结果。

项目通证名：

FIDO

项目通证所在的HECO链上地址：

https://hecoinfo.com/address/0x9c80d1Ff2452dF8c7d061ee277082B6D51b3f6A0

合约所在的Github仓库地址：

暂无

合约在Github中的commit编号：

暂无

合约所在的HECO链上地址：

FIDO.sol : https://hecoinfo.com/address/0x9c80d1Ff2452dF8c7d061ee277082B6D51b3f6A0

MFIL.sol : https://hecoinfo.com/address/0x5CDAFd00AfF95DA3304791A5C9aE00f84506a909

FidoMember.sol : https://hecoinfo.com/address/0xf8118314d8a2a9ac620efb5ae708dc6a54731f93

注：截止撰文时，仅有上述三个合约上链

合约文件及目录结构：

开始审计时合约的文件名及对应的SHA-256哈希值为：

```
Context.sol                :
0x9a3d1e5be0f0ace13e2d9aa1d0a1c3a6574983983ad5de94fc412f878bf7fe89
ERC20.sol                  :
0x8c26e8fa9e13f9dd49a72d9f683aeb1b27073d94926629e6774bcd558653b678
ERC20Burnable.sol          :
0xe5e1be2360243b70d6a2a12bc4f6d364a0da7fec62f7c7caccb9e93583d35337
ERC20Mintable.sol          :
0x9e0af82ac4060a61fe7f018f949dc92f0e7a902900edd97ebcfdeaded8f07595
ERC20Pausable.sol          :
0x743a7b712a14191c93f17c13e03fc8fa0a6fcc82e898bb9a6148350765ea81c2
FIDO-USDT.sol              :
0x3cc47384ba6cbee5e0ffbf64dbe0cb53af031852424b084dbe5c23b513a31829
FIDO.sol                   :
0xaa9997d076160c5dc85d8a8d4edacfc88d6afbf9ee9df56a1018deb8bec76be4
FidoMargin.sol             :
0x9ce458bb0afaf9ff454c273f364b4f921433083407e7c6d99263de2faf7acc9d
FidoMember.sol             :
0xec5581493c6db03689bddc81466abbcd192d88ef7361edb174deaf9f112f8d83
IDOFactory.sol             :
0xadfe68b8715afc6c3f8e52adfbb2fa38b309a3eeb83c82eb2a78aef24449a9e2
IDOInfo.sol                :
0x5fd5c33a0d09e35aedd3f737eec417055e1b00f60ba931e0e5e4ce7e5b9a62fc
```

```
IDOToken.sol              :
0x245a8b998b6ea8aca67a554d41b814711ca011792787abd368a5784e50564cd0
IDOUserRouter.sol         :
0x38858eb853dceca4a621ae0b70c7b5656ae0f6b1da167e1d8b0f2eff5b12885b
MFIL-IDOToken-Factory.sol:
0x48c9bbd1ce6522d26194705a249562cd0ba42690c7bfb8ca954859a27c8206bc
MFIL-IDOToken.sol         :
0x6ded7ea732973012f5a52758222c2a0287451820f1faa896e3499db5ef80a5c6
MFIL.sol                  :
0x45d79b9d3e42e2dd230d48bf277d565180db1609d9260fb737b3fff8eb61ae41
MFILPool.sol              :
0x2be9d371bfcbb8bca9e07c4929a2ad4524fe3203ec2c28e72d76106030706dab
MdexRouter.sol            :
0xdaca46e80b38c739b2f78fa4534beefd502d33444587cadad0630429fce22bec
Migrations.sol            :
0x4fd6092bdfa8b42f19d535c5ac69c4323b0b894717c699e58d5552eeabd04cd4
Ownable.sol               :
0xc4ce2e489b229c0cfe8e13905d187f04526dbda1140856ea9edacca2138e633b
Pausable.sol              :
0x46ec73a6076d161a15e592723707a0a6857d569ef9cfbe881b036d2af89c8e83
ReentrancyGuard.sol       :
0xaa939ebe11a81fcbacbbfc920ab767c0520d48fc9d3d0f8a23a5ac3ac2ffea49
StakeLPRewardPerBlock.sol:
0x1308971a3b7bbd515c17933f43a74ff3874c9b0d95b9dcb137eefcf94315b937
StakeLPRewardPerDay.sol   :
0xd47fa63027d742dfcc50be66b574959fc371a7e0e286b45eebe2444a51c2cadc
StakeRewardPerBlock.sol   :
0xfb527ad127eac435aa25eb82042ec01969f0075501cf9eb8e784acdfcb4b9610
StakeRewardPerDay.sol     :
0x2c8189663fe323e47ecfe7bd2e8195d737bd73d69af5754b82df0eb5c21a823b
StakeTokenPool.sol        :
0x4042e5e13de5163592ada5c2f5c7d9b90f3e803416ec221c06e485dfe0b7f554
IERC20.sol                :
0x0573c2961569aa4906845d0cd428b5b7394956170054ceeaa8f8af96cd44875c
IERC20Mintable.sol        :
0x76d3fb823ed91fab0e9a7ba453b79936a823b2b231801458fcf5bd6991508697
IFidoMember.sol           :
0x6300719088e8f7628a803d35ca229a562e80179498eb716e3173e09b5283e96a
IFidoUsdtLPPool.sol       :
0x505140b94c4b020d6803dac54694c26d90d6f24e54ce3db2993b95282c252de0
IHFIL.sol                 :
0x4c940df88454321edcab4dc8dbfbcff3674ed11aa883ecb40cf75872ab97aed1
IIDOInfo.sol              :
0xa0d230ebb107bfb9f6b1064501886657773f2a4a29ab5c307829c339107cf38b
IIDOToken.sol             :
0xcc0051d7938ebb3dff27f05b2f0ea0cef28337364ad33d619c2d36cbb94dce17
IMFIL.sol                 :
0x95cb2fb46af1643cd56cab7af9c332b3aaab72f471230b2c25b03be1c021610c
IMdexFactory.sol          :
0x2410375170b600d107c94595f655331cc3d0d57fa9561881bb26252f847cfa48
IMdexPair.sol             :
0xf421d6579eb806a61e9184a7bc16fd76428c2ab676788b1a8c199d3c8f518ac0
IRateOracle.sol           :
0x95502495eb910c9af8f0a8a73dc60d46c87d6798a4f8ef1aa3156e2835781275
SafeMath.sol              :
0x4a04d0a20a19e3ef1dcabae9cad9ba006430a4e7eec4d9b519db87999722c98a
TransferHelper.sol        :
0xb036451a96f5bebf2b932c3475af66d73a8dd8a7ad592ffeae59833f2e2698ff
```

```
RateOracle.sol          :
0xc358e644a8b8e9640ed15280f6b52df22930a86bf87261049aee2efa9b0e98fa
```

本次审计的目的是为了审阅Fido项目基于Solidity语言编写的通证发行、质押挖矿、推荐邀请和IDO功能，发现潜在的安全隐患，研究其设计、架构，并试图找到可能存在的漏洞。

我们全面阅读了Fido团队提交的上述合约源码，并仔细审阅了上述代码中可能出现问题的方方面面，对上述合约代码给出了全面、综合的改进意见及评审结果。

— 免责声明

截至本报告发布之日，本报告所阐述的内容仅反映审计团队对当前智能合约安全进展及状况的理解。任何人在接触或使用与本报告相关的服务、产品、协议、平台、或任何物品时，自行承担一切可能产生的冲突、损失、利益及风险，本报告的审计团队概不负责。

本审计不涉及合约的编译器及任何超出智能合约编程语言的领域。所审计的智能合约由引用链下信息或资源所导致的风险及责任不在本审计覆盖的范围之内。

本审计无法详尽查看每一个细节，也无法穷尽每一种可能，因此本报告的审计团队鼓励本合约的开发团队及任何相关利益方对合约进行任何后续的测试及审计。

对任何第三方使用本报告中所提及或涉及的软件、源码、软件库、产品、服务、信息等一切事物所产生的冲突、损失、利益及风险，本审计团队不保证、不承诺也不承担任何责任。

本报告的内容、获取方式、使用以及任何其所涉及的服务或资源都不能作为任何形式的投资、税务、法律、监管及建议等的依据，也不产生相关的责任。

— 审计方式

审计Fido项目的合约代码是为了能清晰地理解该项目的实现方式及运行原理。审计团队对合约代码进行了深入的研究、分析和测试，并收集了详尽的数据。审计团队会在本报告中会详细列举所发现的每个问题、问题所在的源码位置、问题产生的根源以及对问题的描述，并对问题给出相应的改进建议。

灵踪安全审计的流程如下：

1. 背景研究。灵踪安全团队会阅读项目介绍、白皮书、合约源码等一切Fido团队所提供的相关材料及信息，以确保灵踪安全团队理解项目合约的规模、范围及功能。
2. 自动化检测。此步骤主要用自动化工具扫描源码，找到常见的潜在漏洞。
3. 人工审阅合约源码。此步骤由工程师逐行阅读代码，找到潜在的漏洞。
4. 逻辑校对。此步骤审计工程师将对代码的理解与Fido团队提供的材料及信息相比较，检查代码的实现是否符合项目的定义及白皮书等信息中的描述。
5. 测试用例检测。此步骤包括两部分：
   i. 测试用例设计。审计工程师将根据前述步骤对项目背景的理解及合约代码的理解，针对项目可能的执行逻辑及方式设计测试用例。

   ii. 测试范围分析。该步骤会详细检查所设计的测试用例是否覆盖了合约代码的所有逻辑分支，并判断测试用例执行后，合约代码的逻辑是否能得到充分的执行及检查

   iii. 符号执行。该步骤将运行测试用例以测试合约代码所有可能的执行路径。

6. 优化审查。该流程将根据合约的应用场景、调用方式及业界最新的研究成果从可维护性、安全性及可操作性等方面审查合约代码。

— 报告结构

本报告列举的每个问题都被设置了一个安全级别，这些安全级别根据其对合约的影响及安全隐患的大小而定。我们对每个问题都给出了相应的改进建议。为了便于读者阅读，我们分别按主题内容和安全级别这两种方式罗列了所有的问题，并提出了全面增强安全性的建议。

— 引用文档

在审阅过程中，我们参考了与项目相关的文档以加深对项目逻辑、功能及应用的理解。本次报告参阅的文档资料如下：

https://fido.vip/#/

项目白皮书

上述文档被视为本项目代码实现及功能的定义。当我们认为代码实现与文档定义有分歧时，我们及时咨询并与Fido团队进行了沟通和确认。

— 审计结论

经过审计，当前发现的风险数量为：致命风险：0，高危风险：0，中度风险：1，低风险：0。

结论：当前合约代码审计发现风险。

02. 灵踪安全介绍

灵踪安全是一家领先的区块链技术公司，公司为行业企业提供安全审计和咨询方面的服务。灵踪安全研发了自己的一系列合约编写和安全审计标准，为众多客户提供了周到、严谨的服务。

03. 被审计合约项目介绍

本项目为针对FILECOIN的云算力销售而开发的去中心化算力交易平台。

04. 合约主要功能

被审计合约主要实现了下述功能：

- 通证发行：

  通证 `FIDO`：根据业务需要进行增发或者燃烧，可暂停交易，发行上限2亿1千万枚，进行了部分预分配（按周释放/增发）。

  通证 `MFIL`：根据业务需要进行增发或者燃烧，可暂停交易，发行上限20亿枚。
- 质押挖矿：用户质押某种通证得到其它资产奖励
- 推荐邀请：用户可以选择经由推荐人参与项目，也可以不选择。有二级推荐奖励
- IDO：算力商家可以通过本项目平台通过IDO发行通证

注意：本平台中，不管是项目方的FIDO通证、MFIL通证还是算力商家发行的IDO通证，均具有暂停交易的功能。详见“11. 问题详述”。

05. 本审计的主要工作

在审计过程中，灵踪安全着重协助项目方进行了下述工作：

- 审计合约基本功能的逻辑实现是否有错误
- 审计用户质押的资金是否安全
- 审计是否有不必要的权限或者接口
- 审计通证发行是否具有无限发行的可能

06. 风险种类

当前审计采用智能工具静态分析和人工审计相结合的方法，从以下多个风险种类方面对合约源码进行了全方位的审计。

- 重入攻击
- 重放攻击
- 重排攻击
- 注入攻击
- 拒绝服务攻击
- 交易顺序依赖
- 条件竞争攻击

- 权限控制攻击
- 整数上溢/下溢攻击
- 时间戳依赖攻击
- Gas 使用，Gas 限制和循环
- 冗余的回调函数
- 函数状态变量的显式可见性
- 逻辑缺陷
- 未声明的存储指针
- 算术精度误差
- tx.origin 身份验证
- 假充值漏洞
- 变量覆盖
- 设计缺陷
- 潜在后门
- 代币发行
- 管理权限
- 代理升级
- 委托调用插槽共享
- 用户资金安全
- 迁移管理

07. 风险分级

本报告中的每个问题都被设置了一个安全等级，程度由高到低排列如下：

致命 风险及隐患需要立刻解决。

高危 风险及隐患将引发风险及问题，必须解决。

中度 风险及隐患可能导致潜在风险，最终仍然需要解决。

低 风险及隐患主要指各类处理不当或者会引发警告信息的细节，这类问题可以暂时搁置，但建议最终解决。

08. 本审计关注的风险重点

根据本合约的功能及应用场景，我们着重审查了下列功能中可能潜藏的风险。

- 通证发行

我们检查了通证发行是否有不合规的增发接口，以保护投资者的利益和系统的稳定运行。

经审查此功能暂未发现明显风险。

- 权限检查

我们检查了每一个能改变合约状态的函数是否具备合适的权限，重点检查那些必须管理员权限才能操作的函数。

经审查此功能暂未发现风险。

- 通证交易

我们检查了合约中的交易功能是否存在风险。

经审查此功能发现风险，细节请参看“11. 问题详述”。

- 其它

经审查其它功能暂未发现明显风险。

09. 基于风险等级的问题列表

A. 致命风险

- 无

B. 高危风险

- 无

C. 中度风险

- 增加对取值限制的设置

在合约 `IDOUserRouter.sol` 中对下列函数的参数增加取值限制：

在 `changeFidoFeeRate` 函数中，建议对 `_fidoFeeRate` 参数的取值进行限制。

在 `changeInsuranceFeeRate` 函数中，建议对 `_insuranceFeeRate` 参数的取值做出限制。

在 `changeInsuranceFeeRate` 函数中，建议对 `insuranceFeeRate` 参数的取值做出限制。

- 代码优化

在合约 `StakeLPRewardPerBlock.sol` 中，建议将 `caleLiquidity` 函数移至 `MdexRouter.sol` 中去，保持相关实现逻辑的集中性。

- 增加容错性

在合约 `FidoMember.sol` 中，建议 `caleInviteRate` 函数使用一个可升级/替换模式，增强容错性。