



Samurai 钱包安全审计报告



项目概述

此次安全审计项目核心目标是为 Samurai 钱包快速全面的安全审计，检测潜在的威胁点，协力 PlatON 团队一起为客户的资金安全做出最有效的推进，更好的保护广大 Samurai 用户的安全。

前言

感谢 PlatON 项目方对慢雾科技的认可，感谢相关人员的辛苦支持。

审计信息

审计周期：4 个工作日

审计团队：慢雾安全团队

审计时间：2020 年 11 月 20 日 - 2020 年 11 月 25 日

审计文件信息

Samurai 插件钱包文件信息

文件名：samurai-chrome-8.0.10.zip

版本号：8.0.10

SHA256:

8f38556bf5f0c437d2a376c0920f11a4447698e4b0f2457eabbbd3331a90b8e4

项目介绍

Samurai 是基于 MetaMask 开发的浏览器插件钱包，用于适配 Alaya 网络。

主要包含如下功能：

1. 钱包管理：创建钱包，导入钱包，管理钱包。
2. Alaya 网络连接：默认连接 Alaya 网络。
3. 支持 Alaya 网络 ATP 转账。
4. 支持 Alaya 网络 ARC20 代币的管理和转账。
5. 为 DApp 开发者提供 API。

审计结果

(其他未知安全漏洞不包含在本次审计责任范围)

序号	审计大类	审计子类	审计结果
1	交易安全审计	签名安全审计	通过
		转账安全审计	通过
		交易广播安全审计	通过
		假充值审计	通过
		假转账审计	通过
2	私钥管理安全审计	随机数安全审计	通过
		私钥安全审计	通过
		助记词安全审计	通过
		KeyStore 安全审计	通过
3	前端安全审计	DOM XSS 安全审计	通过
		第三方 JS 安全审计	通过
		通信加密与传输安全审计	通过
综合审计结果			通过

最终评级: **优**

免责声明

厦门慢雾科技有限公司(下文简称“慢雾”)仅就本报告出具前已经发生或存在的事实出具本报告,并就此承担相应责任。对于出具报告以后发生或存在的未知漏洞及安全事件,慢雾无法判断其安全状况,亦不对此承担责任。

本报告所作的安全审计分析及其他内容,仅基于信息提供者截至本报告出具时向慢雾提供的文件和资料(简称“已提供资料”)。慢雾假设:已提供资料不存在缺失、被篡改、删减或隐瞒的情形。如已提供资料信息缺失、被篡改、删减、隐瞒或反映的情况与实际情况不符的,慢雾对由此而导致的损失和不利影响不承担任何责任。



官方网址

www.slowmist.com

电子邮箱

team@slowmist.com

微信公众号

