Trail of Bits引用指南

<Title>Trail of Bits完成了对Casper网络Highway协议的审计
<Subtitle>Trail of Bits对Casper的Highway协议在2020年12月所做审计的概述。

Trail of Bits今天表示其已完成对Casper网络的Highway协议的审计。Trail of Bits的审计结果为“未出现高严重性问题，且表现出其已妥善利用了安全防范措施”。

<查看审计结果>

审计范围

Trail of Bits于11月16日至12月1日间进行了审计，其中涉及对CasperLabs网络的Highway共识协议的评估。该审计旨在回答一些关键问题，包括：

- 行为不当的验证者是否将受到惩罚?
- 该系统是否易于受到资源耗竭型攻击?
- 在将单元添加到状态之前，是否先对其进行了适当验证?
- 是否可能出现攻击者对系统做些手脚之后被选举为下一个leader的现象?
- 是否正确实施了LNC验证？LNC验证者的缓冲机制是否合理?

*LNC的全称为“Limited Naivety Criterion”。通过Casper的Highway协议报告了解更多。

审计结果

此次安全审计共有三项发现，一项“参考级严重性”发现和两项“低严重性”发现。

- 未实施LNC验证（参考级严重性）

- Peer不会因为发送无效顶点而受到惩罚（低严重性）
- 限速机制不足（低严重性）

此外，Trail of Bits团队还对提高Highway协议文件本身某些章节的明确性和细节表达提出了建议。

CasperLabs的修复日志

CasperLabs接收并认真读取了Trail of Bits的审计结果，并针对上述三项发现做出调整。

- 未实施LNC验证。**已修复。**
- Peer不会因为发送无效顶点而受到惩罚。**部分修复。**在实际操作中，与该问题相关的风险非常低。
- 限速机制不足。**部分修复。**在实际操作中，与该问题相关的风险非常低。

CasperLabs团队还对Trails of Bits在安全审计中指出的协议文件内有待改进的相关章节进行了调整。

CasperLabs感谢Trail of Bits团队的审计工作和努力。

<查看审计结果>