Security Review of Slashing and DoS Resilience in Grandine

Security Review Report

November 21, 2024

Contents

Disclaimer

THIS AUDIT REPORT HAS BEEN PREPARED FOR THE EXCLUSIVE USE AND BENEFIT OF GRANDINE, MB (THE “CLIENT”) AND SOLELY FOR THE PURPOSE FOR WHICH IT IS PROVIDED. WHILE REASONABLE EFFORTS HAVE BEEN MADE TO ENSURE THE ACCURACY AND COMPLETENESS OF THE FINDINGS AND RECOMMENDATIONS, MATTER LABS DOES NOT GUARANTEE THAT ALL POTENTIAL ISSUES HAVE BEEN IDENTIFIED OR THAT THE INFORMATION PROVIDED IS FREE FROM ERRORS OR OMISSIONS. THE REPORT IS BASED ON THE STATE OF THE CODE AT THE TIME OF THE AUDIT AND MAY NOT REFLECT CHANGES OR UPDATES MADE THEREAFTER.

THE AUDIT REPORT IS PROVIDED “AS IS” WITHOUT ANY WARRANTIES, EXPRESS OR IMPLIED. MATTER LABS EXPRESSLY DISCLAIMS ALL WARRANTIES, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS OF A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THE FINDINGS AND RECOMMENDATIONS CONTAINED IN THIS REPORT ARE INTENDED TO ASSIST IN IMPROVING THE QUALITY AND SECURITY OF THE CODE. HOWEVER, THE IMPLEMENTATION OF THESE RECOMMENDATIONS IS AT THE SOLE DISCRETION AND RISK OF THE CLIENT. MATTER LABS WILL NOT BE LIABLE FOR ANY ACTIONS TAKEN BASED ON THE REPORT, NOR FOR ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES ARISING FROM THE USE AND RELIANCE OF THIS REPORT.

Summary

Scope

This security review examined specific directories and files related to the implementation of slashing mechanisms within the Grandine Ethereum consensus client. The primary focus was on potential DoS attacks, severe flaws in slashing mechanisms, and significant implementation issues that could trigger validator's slashing, whether maliciously or inadvertently. Such incidents could disrupt validator performance, lead to direct financial losses for validator owners, and compromise the overall network stability and economic security.

- **Target release**: https://github.com/grandinetech/grandine/releases/tag/1.0.0.rc0
- **Commit**: 27c20539d685720e38b3f2a600cf08bba30a691b

Security Issues

During our security review, we did not identify any security vulnerabilities or software bugs that could result in the realization of the specific threats under consideration. It is important to note that the review was focused solely on these particular threats. As such, we cannot make any assertions regarding vulnerabilities in other components or those that might lead to different threats.