Monero Distribution Company (Pty) Ltd

Software Security Assessment Services

RandomX Source Code Audit

April 12, 2019
Version: 1.0

Presented by:

Ryan Spanier, Head of Solution Architecture and Research

Nagravision S.A. – Kudelski Security
Route de Genève 22-24
CH-1033 Cheseaux-sur-Lausanne
Switzerland

EXECUTIVE SUMMARY

COMPONENT	DETAILS
Client	Monero Distribution Company (Pty) Ltd
Engagement	RandomX Source Code Audit
Summary	Monero has developed a proof-of-work (PoW) algorithm, called RandomX, that is optimized for general-purpose CPUs. RandomX uses random code execution together with several memory-hard techniques to achieve the following goals: • Prevent the development of a single-chip ASIC • Minimize the efficiency advantage of specialized hardware compared to a general-purpose CPU Monero Research Lab would like a third-party review of the source code of their new RandomX PoW algorithm.
Objectives	In coordination with Monero, Kudelski Security has identified the following engagement objectives: • Help Monero Management, users, and developers to better understand the current risks and security postures of their code base. • Provide a professional opinion on the maturity, adequacy and efficiency of the security measures that are in place within the RandomX proof-of-work (PoW) algorithm. • Identify potential issues and include improvement recommendations based on the result of our review. • Propose prioritized improvements and recommendations to mitigate identified risks and vulnerabilities.
Effort / Duration	To meet Monero objectives, the Kudelski Security team will conduct the following activities: • Security audit of RandomX source code focusing on critical cryptographic components, with a goal of finding security defects, misue of cryptographic components and APIs, unsafe coding risks, and matching the intended behavior as documented in the specifications. • Security audit of the design and protocol as specified in doc/*md files. • Propose improvements in terms of parameter choices and source doce optimization targets, if applicable. • Provide remediation recommendations and perform re-testing. This engagement is estimated to be completed over a period of three (3) weeks. See below for a description of services: • Research, Cryptography, & Security Engineering Services – CHF 17,500 • Project Management Services – CHF 750
Deliverables	Kudelski Security will provide the following deliverables in electronic format: • Executive Summary Presentation designed for Senior Leadership Team / CISO (PDF). • Engagement Findings and Technical Report designed for Managers and Program Owners.
Pricing	Firmed Fixed Price @ CHF 18,250