Trail of Bits

Jim Miller
Engineering Director
james.miller@trailofbits.com

January 30, 2025

Scopely, Inc.

Scopely, Inc. engaged Trail of Bits, Inc. (Trail of Bits), a cybersecurity research and development firm, to review the security of the *Monopoly GO!* pseudorandom number generator (PRNG) architecture. This system is used to generate dice rolls for players. Currently, a small portion of the player base uses "cheating overlays," which provide information about future roll outcomes when different reward multiplier values are selected. Scopely has several proposals for improving the cheating resistance of their PRNG, which Trail of Bits was asked to evaluate.

One consultant conducted the review from December 11, 2024 to December 26, 2024, for a total of two engineer-weeks of effort. The design review focused on the proposed PRNG hardening techniques and their impact on cheating techniques. We also analyzed techniques that can be used by cheating software to recover PRNG state or predict PRNG outputs. While the source code was consulted at several points, the PRNG code was not subjected to a comprehensive security review.

Our review identified one informational issue. The issue does not pose an immediate risk but is instead relevant to security best practices. We found no evidence that the output of the PRNG can be biased or influenced by player rewards or penalties; specifically, we found no evidence that player rewards or penalties can influence or bias the results of dice rolls.

Sincerely,

Jim Miller