

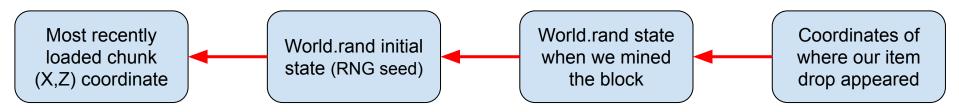
Every time a chunk is loaded, the Woodland Mansion sloppily uses World.rand.setSeed to pick its location.

World.rand is used in hundreds of places, and it can step dozens to thousands of times between the most recent chunk load and when we mine a block.

Dropped items appear at a "random" location within the mined block, that location is picked by asking World.rand for the X, Y, and Z coordinates.

The problem? All of these steps are reversible!

Randar exploit:



Using the overall world generation seed, and the Woodland Mansion check seed, we can guess-and-check all 47k possible X coordinates and compute each's Z.

java.util.Random can be stepped backward as easily as forward. We walk backwards until we find a state that could be from Woodland Mansion generation checks. Our item drop coords are three measurements of the state of World.rand. By using LLL lattice reduction, we can quickly crack the exact state.