Random Numbers – Related CWEs & Example CVEs

- CWE-331 - Insufficient Entropy
    - https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cwe_id=CWE-331
    - https://cwe.mitre.org/data/definitions/331.html
- CWE-332 - Insufficient Entropy in PRNG
    - https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cwe_id=CWE-332
    - https://cwe.mitre.org/data/definitions/332.html
- CWE-335 - Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG)
    - https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cwe_id=CWE-335
    - https://cwe.mitre.org/data/definitions/335.html
- CWE-338 - Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG
    - https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cwe_id=CWE-338
    - https://cwe.mitre.org/data/definitions/338.html