# CWE Detail – CWE-342

## Description

An exact value or random number can be precisely predicted by observing previous values.

## Extended Description

N/A

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2002-1463: Firewall generates easily predictable initial sequence numbers (ISN), which allows remote attackers to spoof connections.

**•** CVE-1999-0074: Listening TCP ports are sequentially allocated, allowing spoofing attacks.

**•** CVE-1999-0077: Predictable TCP sequence numbers allow spoofing.

**•** CVE-2000-0335: DNS resolver uses predictable IDs, allowing a local user to spoof DNS query results.

## Modes of Introduction

**•** Architecture and Design: N/A

**•** Implementation: N/A

## Common Consequences

**•** Impact: Varies by Context — Notes:

## Potential Mitigations

**•** N/A: Increase the entropy used to seed a PRNG. (Effectiveness: N/A)

**•** Architecture and Design: Use products or modules that conform to FIPS 140-2 [REF-267] to avoid obvious entropy problems. Consult FIPS 140-2 Annex C ("Approved Random Number Generators"). (Effectiveness: N/A)

**•** Implementation: Use a PRNG that periodically re-seeds itself using input from high-quality sources, such as hardware devices with high entropy. However, do not re-seed too frequently, or else the entropy source might block. (Effectiveness: N/A)

## Applicable Platforms

**•** None (Class: Not Language-Specific, Prevalence: Undetermined)

## Notes

**•** Maintenance: As of CWE 4.5, terminology related to randomness, entropy, and  
 predictability can vary widely. Within the developer and other  
 communities, "randomness" is used heavily. However, within  
 cryptography, "entropy" is distinct, typically implied as a  
 measurement. There are no commonly-used definitions, even within  
 standards documents and cryptography papers. Future versions of  
 CWE will attempt to define these terms and, if necessary,  
 distinguish between them in ways that are appropriate for  
 different communities but do not reduce the usability of CWE for  
 mapping, understanding, or other scenarios.