# CVE Detail – CVE-2008-2108

The GENERATE\_SEED macro in PHP 4.x before 4.4.8 and 5.x before 5.2.5, when running on 64-bit systems, performs a multiplication that generates a portion of zero bits during conversion due to insufficient precision, which produces 24 bits of entropy and simplifies brute force attacks against protection mechanisms that use the rand and mt\_rand functions.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.88957

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## Mapped CWE(s)

* CWE-331: Insufficient Entropy

## CAPEC(s)

* CAPEC-59: Session Credential Falsification through Prediction

## Affected Products

* cpe:2.3:a:php:php:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:php:php:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:8:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:9:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:6.06:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:7.04:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:7.10:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:canonical:ubuntu\_linux:8.04:\*:\*:\*:-:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:4.0:\*:\*:\*:\*:\*:\*:\*