# CVE Detail – CVE-2019-11495

In Couchbase Server 5.1.1, the cookie used for intra-node communication was not generated securely. Couchbase Server uses erlang:now() to seed the PRNG which results in a small search space for potential random seeds that could then be used to brute force the cookie and execute code against a remote system. This has been fixed in version 6.0.0.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.68173

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## Mapped CWE(s)

* CWE-335: Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG)

## Affected Products

* cpe:2.3:a:couchbase:couchbase\_server:5.1.1:\*:\*:\*:\*:\*:\*:\*