# CVE-2018-16115

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2018-16115 |
| **State** | PUBLIC |
| **Assigner** | cve@mitre.org |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2018-08-29 22:29:00 UTC |
| **Updated** | 2018-11-08 19:40:00 UTC |
| **Description** | Lightbend Akka 2.5.x before 2.5.16 allows message disclosure and modification because of an RNG error. A random numb |

## Risk And Classification

**Problem Types:** CWE-338

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Lightbend | Akka | All | All | All | All |
| Application | Lightbend | Akka | All | All | All | All |

## References

| Reference |
|---|
| Broken random number generators AES128CounterSecureRNG / AES256CounterSecureRNG, Fixed in Akka 2.5.16 • Akka Documentation |
| CVE Program record |
| NVD vulnerability detail |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

980976 Java (maven) Security Update for com.typesafe.akka:akka-actor_2.12 (GHSA-mr95-9rr4-668f)

**CVE.report and Source URL Uptime Status status.cve.report**