# CVE-2016-4970

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2016-4970 |
| **State** | PUBLIC |
| **Assigner** | secalert@redhat.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2017-04-13 14:59:00 UTC |
| **Updated** | 2023-11-07 02:32:00 UTC |
| **Description** | handler/ssl/OpenSslEngine.java in Netty 4.0.x before 4.0.37.Final and 4.1.x before 4.1.1.Final allows remote attackers to ca |

## Risk And Classification

**Problem Types:** CWE-835

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Apache | Cassandra | 3.11.4 | All | All | All |
| Application | Apache | Cassandra | 3.11.4 | All | All | All |
| Application | Netty | Netty | All | All | All | All |
| Application | Netty | Netty | All | All | All | All |
| Application | Redhat | Jboss Data Grid | 7.1 | All | All | All |
| Application | Redhat | Jboss Data Grid | 7.1 | All | All | All |
| Application | Redhat | Jboss Middleware Text-only Advisories | 1.0 | All | All | All |
| Application | Redhat | Jboss Middleware Text-only Advisories | 1.0 | All | All | All |

## References

| Reference | Sourc |
|---|---|
| Red Hat Customer Portal | REDH |
| Pony Mail! | |
| IBM Development Package for Apache Spark CVE-2016-4970 Denial of Service Vulnerability | BID |
| OpenSslEngine writePlaintextData WANT_READ with no data in BIO buffer by Scottmitch · Pull Request #5364 · netty/netty · GitHub | CONF |
| Security Advisories - OpenDaylight Project | CONF |
| Pony Mail! | MLIS |

| | |
|---|---|
| Netty.news: Netty 4.0.37.Final released | CONF |
| 1343616 – (CVE-2016-4970) CVE-2016-4970 netty: Infinite loop vulnerability when handling renegotiation using SslProvider.OpenSsl | CONF |
| Netty.news: Netty 4.1.1.Final released | CONF |
| Red Hat Customer Portal | REDH |
| CVE Program record | CVE.( |
| NVD vulnerability detail | NVD |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.