# CVE-2016-2094

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2016-2094 |
| **State** | PUBLIC |
| **Assigner** | secalert@redhat.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2016-05-06 17:59:00 UTC |
| **Updated** | 2016-05-10 12:11:00 UTC |
| **Description** | The HTTPS NIO Connector allows remote attackers to cause a denial of service (thread consumption) by opening a socket |

## Risk And Classification

**Problem Types:** CWE-399

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Jboss | Enterprise Application Platform | 6.4.6 | All | All | All |
| Application | Jboss | Enterprise Application Platform | 6.4.6 | All | All | All |

## References

| Reference | Sour |
|---|---|
| Red Hat Customer Portal | REDH |
| RHSA-2016:0599 | REDH |
| 1308465 – (CVE-2016-2094) CVE-2016-2094 EAP: HTTPS NIO connector uses no timeout when reading SSL handshake from client | CONI |
| Red Hat Customer Portal | REDH |
| Red Hat Customer Portal | REDH |
| 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.