# CVE-2016-9585

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2016-9585 |
| **State** | PUBLIC |
| **Assigner** | secalert@redhat.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2018-03-09 15:29:00 UTC |
| **Updated** | 2019-10-09 23:20:00 UTC |
| **Description** | Red Hat JBoss EAP version 5 is vulnerable to a deserialization of untrusted data in the JMX endpoint when deserializes the |

## Risk And Classification

**Problem Types:** CWE-502

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Redhat | Jboss Enterprise Application Platform | 5.0.0 | All | All | All |
| Application | Redhat | Jboss Enterprise Application Platform | 5.0.0 | All | All | All |

## References

| Reference | Source | Link |
|---|---|---|
| 1404528 – (CVE-2016-9585) CVE-2016-9585 EAP-5: unsafe deserialization of user credentials by the JMX endpoint | CONFIRM | bugzilla.r |
| Red Hat JBoss Enterprise Application Platform CVE-2016-9585 Remote Denial of Service Vulnerability | BID | www.sec |
| CVE Program record | CVE.ORG | www.cve |
| NVD vulnerability detail | NVD | nvd.nist.g |

No vendor comments have been submitted for this CVE.

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

**Free CVE JSON API** cve.report/api

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