



# CVE-2009-3554

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                        |
|------------------------|------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2009-3554                                                                                                          |
| <b>State</b>           | PUBLIC                                                                                                                 |
| <b>Assigner</b>        | secalert@redhat.com                                                                                                    |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                           |
| <b>Published</b>       | 2009-12-15 18:30:00 UTC                                                                                                |
| <b>Updated</b>         | 2017-08-17 01:31:00 UTC                                                                                                |
| <b>Description</b>     | Twiddle in Red Hat JBoss Enterprise Application Platform (aka JBoss EAP or JBEAP) 4.2 before 4.2.0.CP08 and 4.3 before |

## Risk And Classification

### Problem Types: CWE-200

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                 | Product                                               | Version | Update | Edition | Language |
|-------------|------------------------|-------------------------------------------------------|---------|--------|---------|----------|
| Application | <a href="#">Redhat</a> | <a href="#">Jboss Enterprise Application Platform</a> | 4.2     | All    | All     | All      |
| Application | <a href="#">Redhat</a> | <a href="#">Jboss Enterprise Application Platform</a> | 4.2     | cp01   | All     | All      |
| Application | <a href="#">Redhat</a> | <a href="#">Jboss Enterprise Application Platform</a> | 4.2     | cp02   | All     | All      |
| Application | <a href="#">Redhat</a> | <a href="#">Jboss Enterprise Application Platform</a> | 4.2.0   | cp01   | All     | All      |
| Application | <a href="#">Redhat</a> | <a href="#">Jboss Enterprise Application Platform</a> | 4.2.0   | cp02   | All     | All      |
| Application | <a href="#">Redhat</a> | <a href="#">Jboss Enterprise Application Platform</a> | 4.2.0   | cp03   | All     | All      |
| Application | <a href="#">Redhat</a> | <a href="#">Jboss Enterprise Application Platform</a> | 4.2.0   | cp04   | All     | All      |
| Application | <a href="#">Redhat</a> | <a href="#">Jboss Enterprise Application Platform</a> | 4.2.0   | cp05   | All     | All      |
| Application | <a href="#">Redhat</a> | <a href="#">Jboss Enterprise Application Platform</a> | 4.2.0   | cp06   | All     | All      |
| Application | <a href="#">Redhat</a> | <a href="#">Jboss Enterprise Application Platform</a> | 4.2.0   | cp07   | All     | All      |
| Application | <a href="#">Redhat</a> | <a href="#">Jboss Enterprise Application Platform</a> | 4.2.2   | ga     | All     | All      |
| Application | <a href="#">Redhat</a> | <a href="#">Jboss Enterprise Application Platform</a> | 4.2     | All    | All     | All      |
| Application | <a href="#">Redhat</a> | <a href="#">Jboss Enterprise Application Platform</a> | 4.2     | cp01   | All     | All      |
| Application | <a href="#">Redhat</a> | <a href="#">Jboss Enterprise Application Platform</a> | 4.2     | cp02   | All     | All      |
| Application | <a href="#">Redhat</a> | <a href="#">Jboss Enterprise Application Platform</a> | 4.2.0   | cp01   | All     | All      |
| Application | <a href="#">Redhat</a> | <a href="#">Jboss Enterprise Application Platform</a> | 4.2.0   | cp02   | All     | All      |
| Application | <a href="#">Redhat</a> | <a href="#">Jboss Enterprise Application Platform</a> | 4.2.0   | cp03   | All     | All      |

|             |                        |                                                       |       |      |     |     |
|-------------|------------------------|-------------------------------------------------------|-------|------|-----|-----|
| Application | <a href="#">Redhat</a> | <a href="#">Jboss Enterprise Application Platform</a> | 4.2.0 | cp04 | All | All |
| Application | <a href="#">Redhat</a> | <a href="#">Jboss Enterprise Application Platform</a> | 4.2.0 | cp05 | All | All |
| Application | <a href="#">Redhat</a> | <a href="#">Jboss Enterprise Application Platform</a> | 4.2.0 | cp06 | All | All |
| Application | <a href="#">Redhat</a> | <a href="#">Jboss Enterprise Application Platform</a> | 4.2.0 | cp07 | All | All |
| Application | <a href="#">Redhat</a> | <a href="#">Jboss Enterprise Application Platform</a> | 4.2.2 | ga   | All | All |

## References

| Reference                                                                                                                  | Source  | Link                           |
|----------------------------------------------------------------------------------------------------------------------------|---------|--------------------------------|
| <a href="#">rhnl.redhat.com   Red Hat Support</a>                                                                          | REDHAT  | <a href="#">rhnl.redhat.cc</a> |
| <a href="#">IBM X-Force Exchange</a>                                                                                       | XF      | <a href="#">exchange.xfc</a>   |
| <a href="#">SecurityTracker.com Archives - JBoss Enterprise Application Platform Discloses JMX Password to Local Users</a> | SECTRAK | <a href="#">securitytrack</a>  |
| <a href="#">Bug 532111 – Tracker bug for the EAP 4.2.0.cp08 release for RHEL-5.</a>                                        | CONFIRM | <a href="#">bugzilla.redh</a>  |
| <a href="#">rhnl.redhat.com   Red Hat Support</a>                                                                          | REDHAT  | <a href="#">rhnl.redhat.cc</a> |
| <a href="#">Product Documentation - Red Hat Customer Portal</a>                                                            | CONFIRM | <a href="#">www.redhat.c</a>   |
| <a href="#">About Secunia Research   Flexera</a>                                                                           | SECUNIA | <a href="#">secunia.com</a>    |
| <a href="#">JBoss Enterprise Application Platform Multiple Vulnerabilities</a>                                             | BID     | <a href="#">www.security</a>   |
| <a href="#">rhnl.redhat.com   Red Hat Support</a>                                                                          | REDHAT  | <a href="#">rhnl.redhat.cc</a> |
| <a href="#">jira.jboss.org/jira/browse/JBPAPP-2872</a>                                                                     | CONFIRM | <a href="#">jira.jboss.org</a> |
| <a href="#">539495 – (CVE-2009-3554) CVE-2009-3554 JBoss EAP Twiddle logs the JMX password</a>                             | CONFIRM | <a href="#">bugzilla.redh</a>  |
| <a href="#">rhnl.redhat.com   Red Hat Support</a>                                                                          | REDHAT  | <a href="#">rhnl.redhat.cc</a> |
| <a href="#">CVE Program record</a>                                                                                         | CVE.ORG | <a href="#">www.cve.org</a>    |
| <a href="#">NVD vulnerability detail</a>                                                                                   | NVD     | <a href="#">nvd.nist.gov</a>   |

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)