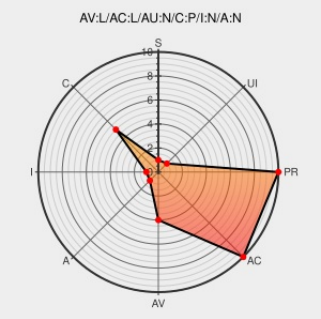
CVE-2009-5066

Published on: 08/13/2012 12:00:00 AM UTC

Last Modified on: 02/13/2023 02:10:39 AM UTC

CVE-2009-5066

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Jboss Community Application Server from Redhat contain the following vulnerability:

twiddle.sh in JBoss AS 5.0 and EAP 5.0 and earlier accepts credentials as command-line arguments, which allows local users to read the credentials by listing the process and its arguments.

CVE-2009-5066 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:0533
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:0194
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:0193
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:0198
Red Hat Customer Portal	web.archive.org	REDHAT RHSA-2013:0196

	text/html Inactive Link Not Archived	
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:0191
oss-security - Re: CVE for JBOSS EAP 5.0(twiddle and jmx invocations) ?	www.openwall.com text/html	MLIST [oss-security] 20120723 Re: CVE for JBOSS EAP 5.0(twiddle and jmx invocations) ?
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:0192
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:0221
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:0195
Security Advisory SA51984 - Red Hat update for JBoss Enterprise Application Platform and JBoss Enterprise Web Platform - Secunia	web.archive.org text/html	SECUNIA 51984
Security Advisory SA52054 - Red Hat update for JBoss Enterprise BRMS Platform - Secunia	web.archive.org text/html	SECUNIA 52054
Securing your JBoss JMX Invoker Layer « Objectopia	objectopia.com text/html	MISC objectopia.com/2009/10/01/securing-jmx-invoker-layer-in-jboss/
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:0197
[JBPAPP-3391] Provide twiddle credentials external to the command line - Red Hat Issue Tracker	issues.jboss.org text/html	CONFIRM issues.jboss.org/browse/JBPAPP-3391?_sscc=t
oss-security - CVE for JBOSS EAP 5.0(twiddle and jmx invocations) ?	www.openwall.com text/html	MLIST [oss-security] 20120720 CVE for JBOSS EAP 5.0(twiddle and jmx invocations) ?

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Jboss Community Application Server	5.0.0	All	All	All
Application	Redhat	Jboss Community Application Server	5.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.0.0	All	All	All

cpe:2.3:a:redhat:jboss_community_application_server:5.0.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:jboss_community_application_server:5.0.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:jboss_enterprise_application_platform:5.0.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:jboss_enterprise_application_platform:5.0.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→