

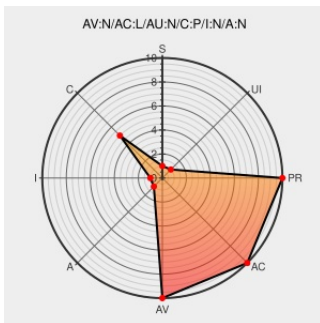


CVE-2009-2747

Published on: 10/30/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:31 PM UTC

CVE-2009-2747

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Websphere Application Server](#) from [Ibm](#) contain the following vulnerability:

The Java Naming and Directory Interface (JNDI) implementation in IBM WebSphere Application Server (WAS) 6.0 before 6.0.2.39, 6.1 before 6.1.0.29, and 7.0 before 7.0.0.7 does not properly restrict access to UserRegistry object methods, which allows remote attackers to obtain sensitive information via a crafted method call.

CVE-2009-2747 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access Vector

NETWORK

Access Complexity

LOW

Authentication

NONE

Confidentiality Impact

PARTIAL

Integrity Impact

NONE

Availability Impact

NONE

CVE References

Description

Tags

Link

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](https://exchange.xforce.ibmcloud.com/text/html)
text/html

[XF was-userregistry-information-disclosure\(54228\)](#)

PK99480: SHIP APAR FIXES FOR H28W700 FIX PACK 7.0.0.7.

[www.ibm.com](http://www.ibm.com/text/html)
text/html

[AIXAPAR PK99480](#)

IBM notice: The page you requested cannot be displayed

[www.ibm.com](http://www.ibm.com/text/html)
text/html
Inactive Link **Not Archived**

[AIXAPAR PK91414](#)

By selecting these links, you may be leaving CVEreport workspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE						
Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	IBM	WebSphere Application Server	6.0	All	All	All
Application	IBM	WebSphere Application Server	6.0.0.1	All	All	All
Application	IBM	WebSphere Application Server	6.0.0.2	All	All	All
Application	IBM	WebSphere Application Server	6.0.0.3	All	All	All
Application	IBM	WebSphere Application Server	6.0.1	All	All	All
Application	IBM	WebSphere Application Server	6.0.1.1	All	All	All
Application	IBM	WebSphere Application Server	6.0.1.11	All	All	All
Application	IBM	WebSphere Application Server	6.0.1.13	All	All	All
Application	IBM	WebSphere Application Server	6.0.1.15	All	All	All
Application	IBM	WebSphere Application Server	6.0.1.17	All	All	All
Application	IBM	WebSphere Application Server	6.0.1.2	All	All	All
Application	IBM	WebSphere Application Server	6.0.1.3	All	All	All
Application	IBM	WebSphere Application Server	6.0.1.5	All	All	All
Application	IBM	WebSphere Application Server	6.0.1.7	All	All	All
Application	IBM	WebSphere Application Server	6.0.1.9	All	All	All
Application	IBM	WebSphere Application Server	6.0.2	All	All	All
Application	IBM	WebSphere Application Server	6.0.2.1	All	All	All
Application	IBM	WebSphere Application Server	6.0.2.11	All	All	All
Application	IBM	WebSphere Application Server	6.0.2.13	All	All	All
Application	IBM	WebSphere Application Server	6.0.2.15	All	All	All
Application	IBM	WebSphere Application Server	6.0.2.17	All	All	All
Application	IBM	WebSphere Application Server	6.0.2.19	All	All	All
Application	IBM	WebSphere Application Server	6.0.2.2	All	All	All
Application	IBM	WebSphere Application Server	6.0.2.22	All	All	All
Application	IBM	WebSphere Application Server	6.0.2.23	All	All	All
Application	IBM	WebSphere Application Server	6.0.2.24	All	All	All
Application	IBM	WebSphere Application Server	6.0.2.25	All	All	All
Application	IBM	WebSphere Application Server	6.0.2.27	All	All	All
Application	IBM	WebSphere Application Server	6.0.2.28	All	All	All
Application	IBM	WebSphere Application Server	6.0.2.29	All	All	All
Application	IBM	WebSphere Application Server	6.0.2.3	All	All	All

[illegible]

[illegible]

Application	lbm	Websphere Application Server	6.0.2.37	All	All	All
Application	lbm	Websphere Application Server	6.0.2.4	All	All	All
Application	lbm	Websphere Application Server	6.0.2.5	All	All	All
Application	lbm	Websphere Application Server	6.0.2.6	All	All	All
Application	lbm	Websphere Application Server	6.0.2.7	All	All	All
Application	lbm	Websphere Application Server	6.0.2.9	All	All	All
Application	lbm	Websphere Application Server	6.1.0	All	All	All
Application	lbm	Websphere Application Server	6.1.0.0	All	All	All
Application	lbm	Websphere Application Server	6.1.0.1	All	All	All
Application	lbm	Websphere Application Server	6.1.0.11	All	All	All
Application	lbm	Websphere Application Server	6.1.0.12	All	All	All
Application	lbm	Websphere Application Server	6.1.0.15	All	All	All
Application	lbm	Websphere Application Server	6.1.0.17	All	All	All
Application	lbm	Websphere Application Server	6.1.0.19	All	All	All
Application	lbm	Websphere Application Server	6.1.0.2	All	All	All
Application	lbm	Websphere Application Server	6.1.0.21	All	All	All
Application	lbm	Websphere Application Server	6.1.0.23	All	All	All
Application	lbm	Websphere Application Server	6.1.0.25	All	All	All
Application	lbm	Websphere Application Server	6.1.0.27	All	All	All
Application	lbm	Websphere Application Server	6.1.0.5	All	All	All
Application	lbm	Websphere Application Server	6.1.0.7	All	All	All
Application	lbm	Websphere Application Server	6.1.0.9	All	All	All
Application	lbm	Websphere Application Server	7.0	All	All	All
Application	lbm	Websphere Application Server	7.0.0.1	All	All	All
Application	lbm	Websphere Application Server	7.0.0.2	All	All	All
Application	lbm	Websphere Application Server	7.0.0.3	All	All	All
Application	lbm	Websphere Application Server	7.0.0.4	All	All	All
Application	lbm	Websphere Application Server	7.0.0.5	All	All	All
Application	lbm	Websphere Application Server	7.0.0.6	All	All	All
cpe:2.3:a:ibm:websphere_application_server:6.0:*:*:*:*:*:						
cpe:2.3:a:ibm:websphere_application_server:6.0.0.1:*:*:*:*:*:						
cpe:2.3:a:ibm:websphere_application_server:6.0.0.2:*:*:*:*:*:						
cpe:2.3:a:ibm:websphere_application_server:6.0.0.3:*:*:*:*:*:						
cpe:2.3:a:ibm:websphere_application_server:6.0.1:*:*:*:*:*:						

cpe:2.3:a:ibm:websphere_application_server:6.0.1.1:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.1.11:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.1.13:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.1.15:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.1.17:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.1.2:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.1.3:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.1.5:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.1.7:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.1.9:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.1:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.11:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.13:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.15:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.17:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.19:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.2:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.22:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.23:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.24:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.25:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.27:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.28:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.29:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.3:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.30:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.31:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.32:*****:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.33:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.35:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.37:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.4:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.5:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.6:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.7:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.9:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.0:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.1:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.11:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.12:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.15:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.17:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.19:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.2:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.21:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.23:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.25:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.27:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.5:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.7:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.9:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.1:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.2:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.3:*****:

cpe:2.3:a:ibm:websphere_application_server:7.0.0.4:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.5:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.6:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.0:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.0.0.1:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.0.0.2:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.0.0.3:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.0.1:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.0.1.1:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.0.1.11:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.0.1.13:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.0.1.15:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.0.1.17:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.0.1.2:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.0.1.3:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.0.1.5:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.0.1.7:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.0.1.9:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.0.2:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.1:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.11:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.13:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.15:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.17:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.19:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.2:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.22:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.23:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.24:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:6.0.2.1:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.25:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.27:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.28:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.29:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.3:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.30:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.31:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.32:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.33:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.35:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.37:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.4:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.5:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.6:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.7:*****:
cpe:2.3:a:ibm:websphere_application_server:6.0.2.9:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.0:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.1:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.11:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.12:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.15:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.17:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.19:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.2:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.21:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.23:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.25:*****:

cpe:2.3:a:ibm:websphere_application_server:6.1.0.27:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.5:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.7:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.9:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.1:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.2:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.3:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.4:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.5:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.6:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)