



# CVE-2010-0714

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2010-0714
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2010-02-26 19:30:00 UTC
<b>Updated</b>	2018-10-10 19:53:00 UTC
<b>Description</b>	Cross-site scripting (XSS) vulnerability in login.jsp in IBM WebSphere Portal, IBM Lotus Web Content Management (WCM)

## Risk And Classification

### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Lotus Quickr	8.0	All	All	All
Application	ibm	Lotus Quickr	8.0.0.2	All	All	All
Application	ibm	Lotus Quickr	8.1	All	All	All
Application	ibm	Lotus Quickr	8.1.1	All	All	All
Application	ibm	Lotus Quickr	8.1.1.1	All	All	All
Application	ibm	Lotus Quickr	8.0	All	All	All
Application	ibm	Lotus Quickr	8.0.0.2	All	All	All
Application	ibm	Lotus Quickr	8.1	All	All	All
Application	ibm	Lotus Quickr	8.1.1	All	All	All
Application	ibm	Lotus Quickr	8.1.1.1	All	All	All
Application	ibm	Lotus Web Content Management	5.1.0.0	All	All	All
Application	ibm	Lotus Web Content Management	5.1.0.1	All	All	All
Application	ibm	Lotus Web Content Management	5.1.0.2	All	All	All
Application	ibm	Lotus Web Content Management	5.1.0.3	All	All	All
Application	ibm	Lotus Web Content Management	5.1.0.4	All	All	All
Application	ibm	Lotus Web Content Management	5.1.0.5	All	All	All
Application	ibm	Lotus Web Content Management	6.0.0.0	All	All	All





Application	lbn	Lotus Workplace Web Content Management	5.1.0.5	All	All	All
Application	lbn	Lotus Workplace Web Content Management	6.0.0.0	All	All	All
Application	lbn	Lotus Workplace Web Content Management	6.0.0.1	All	All	All
Application	lbn	Lotus Workplace Web Content Management	6.0.0.2	All	All	All
Application	lbn	Lotus Workplace Web Content Management	6.0.0.3	All	All	All
Application	lbn	Lotus Workplace Web Content Management	6.0.0.4	All	All	All
Application	lbn	Lotus Workplace Web Content Management	6.0.1.0	All	All	All
Application	lbn	Lotus Workplace Web Content Management	6.0.1.1	All	All	All
Application	lbn	Lotus Workplace Web Content Management	6.0.1.2	All	All	All
Application	lbn	Lotus Workplace Web Content Management	6.0.1.3	All	All	All
Application	lbn	Lotus Workplace Web Content Management	6.0.1.4	All	All	All
Application	lbn	Lotus Workplace Web Content Management	6.0.1.5	All	All	All
Application	lbn	Lotus Workplace Web Content Management	6.0.1.6	All	All	All
Application	lbn	Lotus Workplace Web Content Management	6.0.1.7	All	All	All
Application	lbn	Lotus Workplace Web Content Management	6.1.0.0	All	All	All
Application	lbn	Lotus Workplace Web Content Management	6.1.0.1	All	All	All
Application	lbn	Lotus Workplace Web Content Management	6.1.0.2	All	All	All
Application	lbn	Lotus Workplace Web Content Management	6.1.0.3	All	All	All
Application	lbn	Lotus Workplace Web Content Management	6.1.5.0	All	All	All
Application	lbn	Websphere Portal	5.1.0.0	All	All	All
Application	lbn	Websphere Portal	5.1.0.1	All	All	All
Application	lbn	Websphere Portal	5.1.0.2	All	All	All
Application	lbn	Websphere Portal	5.1.0.3	All	All	All
Application	lbn	Websphere Portal	5.1.0.4	All	All	All
Application	lbn	Websphere Portal	5.1.0.5	All	All	All
Application	lbn	Websphere Portal	6.0.0.0	All	All	All
Application	lbn	Websphere Portal	6.0.0.1	All	All	All
Application	lbn	Websphere Portal	6.0.0.2	All	All	All
Application	lbn	Websphere Portal	6.0.0.3	All	All	All
Application	lbn	Websphere Portal	6.0.0.4	All	All	All
Application	lbn	Websphere Portal	6.0.1.0	All	All	All
Application	lbn	Websphere Portal	6.0.1.1	All	All	All
Application	lbn	Websphere Portal	6.0.1.2	All	All	All
Application	lbn	Websphere Portal	6.0.1.3	All	All	All
Application	lbn	Websphere Portal	6.0.1.4	All	All	All
Application	lbn	Websphere Portal	6.0.1.5	All	All	All

Application	ibm	Websphere Portal	6.0.1.6	All	All	All
Application	ibm	Websphere Portal	6.0.1.7	All	All	All
Application	ibm	Websphere Portal	6.1.0.0	All	All	All
Application	ibm	Websphere Portal	6.1.0.1	All	All	All
Application	ibm	Websphere Portal	6.1.0.2	All	All	All
Application	ibm	Websphere Portal	6.1.0.3	All	All	All
Application	ibm	Websphere Portal	6.1.5.0	All	All	All
Application	ibm	Websphere Portal	5.1.0.0	All	All	All
Application	ibm	Websphere Portal	5.1.0.1	All	All	All
Application	ibm	Websphere Portal	5.1.0.2	All	All	All
Application	ibm	Websphere Portal	5.1.0.3	All	All	All
Application	ibm	Websphere Portal	5.1.0.4	All	All	All
Application	ibm	Websphere Portal	5.1.0.5	All	All	All
Application	ibm	Websphere Portal	6.0.0.0	All	All	All
Application	ibm	Websphere Portal	6.0.0.1	All	All	All
Application	ibm	Websphere Portal	6.0.0.2	All	All	All
Application	ibm	Websphere Portal	6.0.0.3	All	All	All
Application	ibm	Websphere Portal	6.0.0.4	All	All	All
Application	ibm	Websphere Portal	6.0.1.0	All	All	All
Application	ibm	Websphere Portal	6.0.1.1	All	All	All
Application	ibm	Websphere Portal	6.0.1.2	All	All	All
Application	ibm	Websphere Portal	6.0.1.3	All	All	All
Application	ibm	Websphere Portal	6.0.1.4	All	All	All
Application	ibm	Websphere Portal	6.0.1.5	All	All	All
Application	ibm	Websphere Portal	6.0.1.6	All	All	All
Application	ibm	Websphere Portal	6.0.1.7	All	All	All
Application	ibm	Websphere Portal	6.1.0.0	All	All	All
Application	ibm	Websphere Portal	6.1.0.1	All	All	All
Application	ibm	Websphere Portal	6.1.0.2	All	All	All
Application	ibm	Websphere Portal	6.1.0.3	All	All	All
Application	ibm	Websphere Portal	6.1.5.0	All	All	All

## References

### Reference

IBM WebSphere Portal Input Validation Hole in 'login.jsp' Permits Cross-Site Scripting Attacks - SecurityTracker

SecurityFocus

Multiple IBM Products Login Page Cross Site Scripting Vulnerability

IBM X-Force Exchange

IBM - Security Risk with Fix Available: Web Content Management login page vulnerable to cross site scripting attacks, also affects WebSphere

Hacktics :: Advisories :: Cross Site Scripting Vulnerability in IBM WebSphere Portal Server & Lotus WCM

IBM notice: The page you requested cannot be displayed

CVE Program record

NVD vulnerability detail



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](#)