

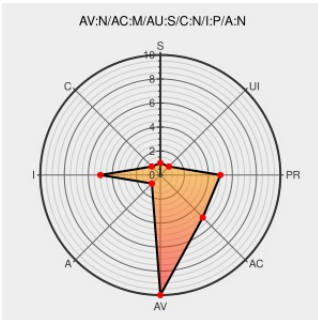


CVE-2013-4005

Published on: 08/21/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:29 PM UTC

CVE-2013-4005

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

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

Cross-site scripting (XSS) vulnerability in the Administrative console in IBM WebSphere Application Server (WAS) 6.1 before 6.1.0.47, 7.0 before 7.0.0.31, 8.0 before 8.0.0.7, and 8.5 before 8.5.5.1 allows remote authenticated users to inject arbitrary web script or HTML via unspecified fields.

CVE-2013-4005 has been assigned by [psirt@us.ibm.com](#) to track the vulnerability

CVSS2 Score: **3.5 - LOW**

Access Vector

NETWORK

Access Complexity

MEDIUM

Authentication

SINGLE

Confidentiality Impact

NONE

Integrity Impact

PARTIAL

Availability Impact

NONE

CVE References

Description

Tags

Link

IBM X-Force Exchange

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

[XF was-cve20134005-xss\(85270\)](#)

IBM Security Bulletin: Potential Security Vulnerabilities fixed in IBM WebSphere Application Server 8.0.0.7 - United States

[Vendor Advisory](#)
[www-01.ibm.com](#)
[text/html](#)

[CONFIRM www-01.ibm.com/support/docview.wss?uid=swg21644047](#)

IBM WebSphere Application Server Input Validation Flaw in Administrative Console Permits Cross-Site Scripting Attacks - SecurityTracker

[www.securitytracker.com](#)
[text/html](#)

[SECTRAK 1028932](#)

IBM notice: The page you requested cannot be displayed

[www-01.ibm.com](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[AIXAPAR PM88208](#)

By selecting these links, you may be leaving CVEreport webspace. 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	6.1	All	All	All
Application	Ibm	Websphere Application Server	6.1.0	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.0	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.1	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.11	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.12	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.13	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.14	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.15	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.17	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.19	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.2	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.21	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.23	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.25	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.27	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.29	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.3	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.31	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.33	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.35	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.37	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.39	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.41	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.43	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.45	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.5	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.7	All	All	All

[illegible]

[illegible]

[illegible]

Application	ibm	Websphere Application Server	7.0.0.8	All	All	All
Application	ibm	Websphere Application Server	7.0.0.9	All	All	All
Application	ibm	Websphere Application Server	8.0.0.0	All	All	All
Application	ibm	Websphere Application Server	8.0.0.1	All	All	All
Application	ibm	Websphere Application Server	8.0.0.2	All	All	All
Application	ibm	Websphere Application Server	8.0.0.3	All	All	All
Application	ibm	Websphere Application Server	8.0.0.4	All	All	All
Application	ibm	Websphere Application Server	8.0.0.5	All	All	All
Application	ibm	Websphere Application Server	8.0.0.6	All	All	All
Application	ibm	Websphere Application Server	8.5.0.0	All	All	All
Application	ibm	Websphere Application Server	8.5.0.1	All	All	All
Application	ibm	Websphere Application Server	8.5.0.2	All	All	All
cpe:2.3:a:ibm:websphere_application_server:6.1:*:*:*:*:*:						
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:6.1.0.13:*:*:*:*:*:						
cpe:2.3:a:ibm:websphere_application_server:6.1.0.14:*:*:*:*:*:						
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:6.1.0.29:*:*:*:*:*:						
cpe:2.3:a:ibm:websphere_application_server:6.1.0.3:*:*:*:*:*:						
cpe:2.3:a:ibm:websphere application server:6.1.0.31:*:*:*:*:*:						

cpe:2.3:a:ibm:websphere_application_server:6.1.0.33:****:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.35:****:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.37:****:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.39:****:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.41:****:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.43:****:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.45:****:*:*:
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:6.1.1:****:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.13:****:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.14:****:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.3:****:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.5:****:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.6:****:*:*:
cpe:2.3:a:ibm:websphere_application_server:6.1.7:****:*:*:
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:7.0.0.10:****:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.11:****:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.12:****:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.13:****:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.14:****:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.15:****:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.16:****:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.17:****:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.18:****:*:*:

cpe:2.3:a:ibm:websphere_application_server:7.0.0.19:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.2:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.21:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.22:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.23:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.24:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.25:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.27:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.29:*****:
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:7.0.0.7:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.8:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.9:*****:
cpe:2.3:a:ibm:websphere_application_server:8.0.0.0:*****:
cpe:2.3:a:ibm:websphere_application_server:8.0.0.1:*****:
cpe:2.3:a:ibm:websphere_application_server:8.0.0.2:*****:
cpe:2.3:a:ibm:websphere_application_server:8.0.0.3:*****:
cpe:2.3:a:ibm:websphere_application_server:8.0.0.4:*****:
cpe:2.3:a:ibm:websphere_application_server:8.0.0.5:*****:
cpe:2.3:a:ibm:websphere_application_server:8.0.0.6:*****:
cpe:2.3:a:ibm:websphere_application_server:8.5.0.0:*****:
cpe:2.3:a:ibm:websphere_application_server:8.5.0.1:*****:
cpe:2.3:a:ibm:websphere_application_server:8.5.0.2:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1:*****:
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:6.1.0.1:*****:
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:6.1.0.13:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.14:*****:
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:6.1.0.29:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.3:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.31:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.33:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.35:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.37:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.39:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.41:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.43:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.45:*****:
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:6.1.1:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.13:*****:

cpe:2.3:a:ibm:websphere_application_server:6.1.14:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.3:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.5:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.6:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.7:*****:
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:7.0.0.10:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.11:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.12:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.13:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.14:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.15:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.16:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.17:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.18:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.19:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.2:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.21:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.22:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.23:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.24:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.25:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.27:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.29:*****:
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:7.0.0.6:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.7:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.8:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.9:*****:
cpe:2.3:a:ibm:websphere_application_server:8.0.0.0:*****:
cpe:2.3:a:ibm:websphere_application_server:8.0.0.1:*****:
cpe:2.3:a:ibm:websphere_application_server:8.0.0.2:*****:
cpe:2.3:a:ibm:websphere_application_server:8.0.0.3:*****:
cpe:2.3:a:ibm:websphere_application_server:8.0.0.4:*****:
cpe:2.3:a:ibm:websphere_application_server:8.0.0.5:*****:
cpe:2.3:a:ibm:websphere_application_server:8.0.0.6:*****:
cpe:2.3:a:ibm:websphere_application_server:8.5.0.0:*****:
cpe:2.3:a:ibm:websphere_application_server:8.5.0.1:*****:
cpe:2.3:a:ibm:websphere_application_server:8.5.0.2:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)