

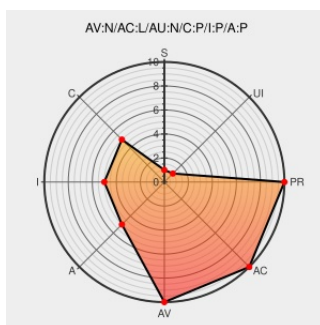


CVE-2009-2085

Published on: 08/13/2009 12:00:00 AM UTC

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

CVE-2009-2085

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

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

The Security component in IBM WebSphere Application Server (WAS) 6.1 before 6.1.0.25 and 7.0 before 7.0.0.5 does not properly handle use of Identity Assertion with CSiv2 Security, which allows remote attackers to bypass intended CSiv2 access restrictions via vectors involving Enterprise JavaBeans (EJB).

CVE-2009-2085 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

IBM Fix list for IBM WebSphere Application Server V6.1 - United States

[Patch](#)
[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[CONFIRM](#) [www-01.ibm.com/support/docview.wss?uid=swg27007951](#)

IBM X-Force Exchange

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

[XF was-csiv2-security-bypass\(52076\)](#)

IBM notice: The page you requested cannot be displayed

[www-1.ibm.com](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[AIXAPAR PK83097](#)

IBM Fix list for IBM WebSphere Application Server V7.0 - United States

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

[CONFIRM](#) [www-01.ibm.com/support/docview.wss?uid=swg27014463](#)

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	6.1.0.10	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	6.1.0.16	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.17	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.18	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	6.1.0.20	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.21	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.22	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.23	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.24	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.3	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.4	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.5	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.6	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.7	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.8	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.9	All	All	All

Application	Ibm	Websphere Application Server	7.0	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.1	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.3	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.4	All	All	All
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	6.1.0.10	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	6.1.0.16	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.17	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.18	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	6.1.0.20	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.21	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.22	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.23	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.24	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.3	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.4	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.5	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.6	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.7	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.8	All	All	All
Application	Ibm	Websphere Application Server	6.1.0.9	All	All	All
Application	Ibm	Websphere Application Server	7.0	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.1	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.3	All	All	All
Application	Ibm	Websphere Application Server	7.0.0.4	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:*****:
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:6.1.0.10:*****:
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:6.1.0.16:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.17:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.18:*****:
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:6.1.0.20:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.21:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.22:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.23:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.24:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.3:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.4:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.5:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.6:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.7:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.8:*****:
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:7.0.0.3:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.4:*****:
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:6.1.0.10:*****:
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:6.1.0.16:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.17:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.18:*****:
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:6.1.0.20:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.21:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.22:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.23:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.24:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.3:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.4:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.5:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.6:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.7:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.8:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.9:*****:

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:7.0.0.3:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.4:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)