

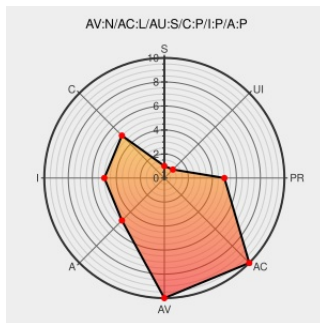


CVE-2011-1321

Published on: 03/08/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:17 PM UTC

CVE-2011-1321

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

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

The AuthCache purge implementation in the Security component in IBM WebSphere Application Server (WAS) 6.1.0.x before 6.1.0.37 and 7.x before 7.0.0.15 does not purge a user from the PlatformCredential cache, which might allow remote authenticated users to gain privileges by leveraging a group membership specified in an old RACF Object

(aka RACO).

CVE-2011-1321 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
PM24668: UNABLE TO PURGE A USER IN THE AUTHCACHE.	www-01.ibm.com text/html	AIXAPAR PM24668
IBM Fix list for IBM WebSphere Application Server V7.0 - United States	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	6.1.0	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	6.1.0.15	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	6.1.0.5	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.7	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	7.0.0.11	All	All	All
Application	IBM	WebSphere Application Server	7.0.0.13	All	All	All
Application	IBM	WebSphere Application Server	7.0.0.2	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	7.0.0.5	All	All	All
Application	IBM	WebSphere Application Server	7.0.0.6	All	All	All
Application	IBM	WebSphere Application Server	7.0.0.7	All	All	All
Application	IBM	WebSphere Application Server	7.0.0.8	All	All	All

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:6.1.0.29:*****:
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:6.1.0.5:*****:
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:7.0.0.11:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.13:*****:
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: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: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:6.1.0.29:*****:
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:6.1.0.5:*****:
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:7.0.0.11:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.13:*****:

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: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:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)