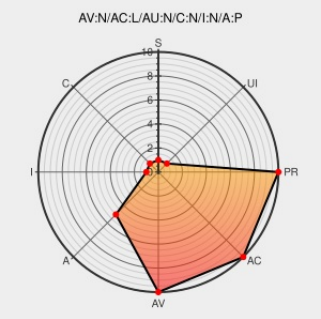
CVE-2011-1313

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

Last Modified on: 03/23/2021 11:23:15 PM UTC

CVE-2011-1313

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Websphere Application Server from Ibm contain the following vulnerability:

Double free vulnerability in IBM WebSphere Application Server (WAS) 6.1.0.x before 6.1.0.35 and 7.x before 7.0.0.15 allows remote backend IIOP servers to cause a denial of service (S0C4 ABEND and storage corruption) by rejecting IIOP requests at opportunistic time instants, as demonstrated by requests associated with an ORB_Request::getACRWorkElementPtr function call.

CVE-2011-1313 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
IBM PM17170: S0C4 IN METHODS SUCH AS ORB_REQUEST::GETACRWORKELEMENTPTR() DUE TO DOUBLE FREE OF BBOOORBR - United States	Patch, Vendor Advisory, www-01.ibm.com, text/html	AIXAPAR PM17170
IBM Fix list for IBM WebSphere Application Server V7.0 - United States	Patch, Vendor Advisory, www-01.ibm.com, text/html	CONFIRM www-01.ibm.com/support/docview.wss?uid=swg27014463

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	6.1.0.5	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
Application	Ibm	Websphere Application Server	7.0.0.9	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	6.1.0.15	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	6.1.0.5	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
Application	Ibm	Websphere Application Server	7.0.0.9	All	All	All

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:6.1.0.5:*:*:*:*:*:*:*:

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:6.1.0.5:*:*:*:*:*:*:*:

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→