



[MITRE](#)
[NVD](#)
[CVE.ORG](#)
[JSON API](#)
[Print: PDF](#)

CVE	CVE-2014-3065
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-12-02 01:59:00 UTC
Updated	2015-03-18 02:00:00 UTC
Description	Unspecified vulnerability in IBM Java Runtime Environment (JRE) 7 R1 before SR2 (7.1.2.0), 7 before SR8 (7.0.8.0), 6 R1 before SR2 (6.0.2.0), 6 before SR8 (6.0.8.0), 5 R1 before SR2 (5.0.2.0), 5 before SR8 (5.0.8.0), 4 R1 before SR2 (4.0.2.0), 4 before SR8 (4.0.8.0), 3 R1 before SR2 (3.0.2.0), 3 before SR8 (3.0.8.0), 2 R1 before SR2 (2.0.2.0), 2 before SR8 (2.0.8.0), 1 R1 before SR2 (1.0.2.0), 1 before SR8 (1.0.8.0), or 1 R1 before SR2 (1.0.2.0), 1 before SR8 (1.0.8.0), could allow remote attackers to execute arbitrary code via crafted Java archive files.

Problem Types: CWE-94

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Java	5.0.0.0	All	All	All
Application	Ibm	Java	5.0.11.0	All	All	All
Application	Ibm	Java	5.0.11.1	All	All	All
Application	Ibm	Java	5.0.11.2	All	All	All
Application	Ibm	Java	5.0.12.0	All	All	All
Application	Ibm	Java	5.0.12.1	All	All	All
Application	Ibm	Java	5.0.12.2	All	All	All
Application	Ibm	Java	5.0.12.3	All	All	All
Application	Ibm	Java	5.0.12.4	All	All	All
Application	Ibm	Java	5.0.12.5	All	All	All
Application	Ibm	Java	5.0.13.0	All	All	All
Application	Ibm	Java	5.0.14.0	All	All	All
Application	Ibm	Java	5.0.15.0	All	All	All
Application	Ibm	Java	5.0.16.0	All	All	All
Application	Ibm	Java	5.0.16.1	All	All	All
Application	Ibm	Java	5.0.16.2	All	All	All
Application	Ibm	Java	5.0.16.3	All	All	All

Application	lbm	Java	6.0.0.0	All	All	All
Application	lbm	Java	6.0.1.0	All	All	All
Application	lbm	Java	6.0.10.0	All	All	All
Application	lbm	Java	6.0.10.1	All	All	All
Application	lbm	Java	6.0.11.0	All	All	All
Application	lbm	Java	6.0.12.0	All	All	All
Application	lbm	Java	6.0.13.0	All	All	All
Application	lbm	Java	6.0.13.1	All	All	All
Application	lbm	Java	6.0.13.2	All	All	All
Application	lbm	Java	6.0.14.0	All	All	All
Application	lbm	Java	6.0.2.0	All	All	All
Application	lbm	Java	6.0.3.0	All	All	All
Application	lbm	Java	6.0.4.0	All	All	All
Application	lbm	Java	6.0.5.0	All	All	All
Application	lbm	Java	6.0.6.0	All	All	All
Application	lbm	Java	6.0.7.0	All	All	All
Application	lbm	Java	6.0.8.0	All	All	All
Application	lbm	Java	6.0.8.1	All	All	All
Application	lbm	Java	6.0.9.0	All	All	All
Application	lbm	Java	6.0.9.1	All	All	All
Application	lbm	Java	6.0.9.2	All	All	All
Application	lbm	Java	7.0.0.0	All	All	All
Application	lbm	Java	7.0.1.0	All	All	All
Application	lbm	Java	7.0.2.0	All	All	All
Application	lbm	Java	7.0.3.0	All	All	All
Application	lbm	Java	7.0.4.0	All	All	All
Application	lbm	Java	7.0.4.1	All	All	All
Application	lbm	Java	7.0.4.2	All	All	All
Application	lbm	Java	7.0.5.0	All	All	All
Application	lbm	Java	5.0.0.0	All	All	All
Application	lbm	Java	5.0.11.0	All	All	All
Application	lbm	Java	5.0.11.1	All	All	All
Application	lbm	Java	5.0.11.2	All	All	All
Application	lbm	Java	5.0.12.0	All	All	All
Application	lbm	Java	5.0.12.1	All	All	All

Application	lbm	Java	5.0.12.2	All	All	All
Application	lbm	Java	5.0.12.3	All	All	All
Application	lbm	Java	5.0.12.4	All	All	All
Application	lbm	Java	5.0.12.5	All	All	All
Application	lbm	Java	5.0.13.0	All	All	All
Application	lbm	Java	5.0.14.0	All	All	All
Application	lbm	Java	5.0.15.0	All	All	All
Application	lbm	Java	5.0.16.0	All	All	All
Application	lbm	Java	5.0.16.1	All	All	All
Application	lbm	Java	5.0.16.2	All	All	All
Application	lbm	Java	5.0.16.3	All	All	All
Application	lbm	Java	6.0.0.0	All	All	All
Application	lbm	Java	6.0.1.0	All	All	All
Application	lbm	Java	6.0.10.0	All	All	All
Application	lbm	Java	6.0.10.1	All	All	All
Application	lbm	Java	6.0.11.0	All	All	All
Application	lbm	Java	6.0.12.0	All	All	All
Application	lbm	Java	6.0.13.0	All	All	All
Application	lbm	Java	6.0.13.1	All	All	All
Application	lbm	Java	6.0.13.2	All	All	All
Application	lbm	Java	6.0.14.0	All	All	All
Application	lbm	Java	6.0.2.0	All	All	All
Application	lbm	Java	6.0.3.0	All	All	All
Application	lbm	Java	6.0.4.0	All	All	All
Application	lbm	Java	6.0.5.0	All	All	All
Application	lbm	Java	6.0.6.0	All	All	All
Application	lbm	Java	6.0.7.0	All	All	All
Application	lbm	Java	6.0.8.0	All	All	All
Application	lbm	Java	6.0.8.1	All	All	All
Application	lbm	Java	6.0.9.0	All	All	All
Application	lbm	Java	6.0.9.1	All	All	All
Application	lbm	Java	6.0.9.2	All	All	All
Application	lbm	Java	7.0.0.0	All	All	All
Application	lbm	Java	7.0.1.0	All	All	All
Application	lbm	Java	7.0.2.0	All	All	All
Application	lbm	Java	7.0.3.0	All	All	All

Application	Ibm	Java	7.0.3.0	All	All	All
Application	Ibm	Java	7.0.4.0	All	All	All
Application	Ibm	Java	7.0.4.1	All	All	All
Application	Ibm	Java	7.0.4.2	All	All	All
Application	Ibm	Java	7.0.5.0	All	All	All

References	
Reference	Source
IBM IV66045: FIX SECURITY VULNERABILITY CVE-2014-3065 - United States	AIXAPAR
[security-announce] SUSE-SU-2014:1526-1: important: Security update for	SUSE
IBM Java SDK CVE-2014-3065 Local Arbitrary Code Execution Vulnerability	BID
Red Hat Customer Portal	REDHAT
[security-announce] SUSE-SU-2015:0344-1: important: Security update for	SUSE
Red Hat Customer Portal	REDHAT
[security-announce] SUSE-SU-2015:0376-1: important: Security update for	SUSE
[security-announce] SUSE-SU-2015:0392-1: important: Security update for	SUSE
Red Hat Customer Portal	REDHAT
IBM IV66044: FIX SECURITY VULNERABILITY CVE-2014-3065 - United States	AIXAPAR
Red Hat Customer Portal	REDHAT
Red Hat Customer Portal	REDHAT
IBM Security Bulletin: Multiple vulnerabilities in current releases of the IBM® SDK, Java™ Technology Edition - United States	CONFIRM
[security-announce] SUSE-SU-2015:0345-1: important: Security update for	SUSE
[security-announce] SUSE-SU-2014:1549-1: important: Security update for	SUSE
Red Hat Customer Portal	REDHAT
Bug 1162554 – CVE-2014-3065 IBM JDK: privilege escalation via shared class cache	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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