



CVE-2014-0878

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

Summary

CVE	CVE-2014-0878
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-05-26 19:55:00 UTC
Updated	2017-08-29 01:34:00 UTC
Description	The IBMSecureRandom component in the IBMJCE and IBMSecureRandom cryptographic providers in IBM SDK Java Tech

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

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

Application	Ibm	Java Sdk	5.0.16.4	All	All	All
Application	Ibm	Java Sdk	5.0.16.5	All	All	All
Application	Ibm	Java Sdk	6.0.0.0	All	All	All
Application	Ibm	Java Sdk	6.0.1.0	All	All	All
Application	Ibm	Java Sdk	6.0.10.0	All	All	All
Application	Ibm	Java Sdk	6.0.10.1	All	All	All
Application	Ibm	Java Sdk	6.0.11.0	All	All	All
Application	Ibm	Java Sdk	6.0.12.0	All	All	All
Application	Ibm	Java Sdk	6.0.13.0	All	All	All
Application	Ibm	Java Sdk	6.0.13.1	All	All	All
Application	Ibm	Java Sdk	6.0.13.2	All	All	All
Application	Ibm	Java Sdk	6.0.14.0	All	All	All
Application	Ibm	Java Sdk	6.0.15.0	All	All	All
Application	Ibm	Java Sdk	6.0.15.1	All	All	All
Application	Ibm	Java Sdk	6.0.2.0	All	All	All
Application	Ibm	Java Sdk	6.0.3.0	All	All	All
Application	Ibm	Java Sdk	6.0.4.0	All	All	All
Application	Ibm	Java Sdk	6.0.5.0	All	All	All
Application	Ibm	Java Sdk	6.0.6.0	All	All	All
Application	Ibm	Java Sdk	6.0.7.0	All	All	All
Application	Ibm	Java Sdk	6.0.8.0	All	All	All
Application	Ibm	Java Sdk	6.0.8.1	All	All	All
Application	Ibm	Java Sdk	6.0.9.0	All	All	All
Application	Ibm	Java Sdk	6.0.9.1	All	All	All
Application	Ibm	Java Sdk	6.0.9.2	All	All	All
Application	Ibm	Java Sdk	7.0.0.0	All	All	All
Application	Ibm	Java Sdk	7.0.1.0	All	All	All
Application	Ibm	Java Sdk	7.0.2.0	All	All	All
Application	Ibm	Java Sdk	7.0.3.0	All	All	All
Application	Ibm	Java Sdk	7.0.4.0	All	All	All
Application	Ibm	Java Sdk	7.0.4.1	All	All	All
Application	Ibm	Java Sdk	7.0.4.2	All	All	All
Application	Ibm	Java Sdk	7.0.5.0	All	All	All
Application	Ibm	Java Sdk	7.0.6.0	All	All	All
Application	Ibm	Java Sdk	7.0.6.1	All	All	All

Application	Ibm	Java Sdk	7.1.0.0	All	All	All
Application	Ibm	Java Sdk	5.0.0.0	All	All	All
Application	Ibm	Java Sdk	5.0.11.0	All	All	All
Application	Ibm	Java Sdk	5.0.11.1	All	All	All
Application	Ibm	Java Sdk	5.0.11.2	All	All	All
Application	Ibm	Java Sdk	5.0.12.0	All	All	All
Application	Ibm	Java Sdk	5.0.12.1	All	All	All
Application	Ibm	Java Sdk	5.0.12.2	All	All	All
Application	Ibm	Java Sdk	5.0.12.3	All	All	All
Application	Ibm	Java Sdk	5.0.12.4	All	All	All
Application	Ibm	Java Sdk	5.0.12.5	All	All	All
Application	Ibm	Java Sdk	5.0.13.0	All	All	All
Application	Ibm	Java Sdk	5.0.14.0	All	All	All
Application	Ibm	Java Sdk	5.0.15.0	All	All	All
Application	Ibm	Java Sdk	5.0.16.0	All	All	All
Application	Ibm	Java Sdk	5.0.16.1	All	All	All
Application	Ibm	Java Sdk	5.0.16.2	All	All	All
Application	Ibm	Java Sdk	5.0.16.3	All	All	All
Application	Ibm	Java Sdk	5.0.16.4	All	All	All
Application	Ibm	Java Sdk	5.0.16.5	All	All	All
Application	Ibm	Java Sdk	6.0.0.0	All	All	All
Application	Ibm	Java Sdk	6.0.1.0	All	All	All
Application	Ibm	Java Sdk	6.0.10.0	All	All	All
Application	Ibm	Java Sdk	6.0.10.1	All	All	All
Application	Ibm	Java Sdk	6.0.11.0	All	All	All
Application	Ibm	Java Sdk	6.0.12.0	All	All	All
Application	Ibm	Java Sdk	6.0.13.0	All	All	All
Application	Ibm	Java Sdk	6.0.13.1	All	All	All
Application	Ibm	Java Sdk	6.0.13.2	All	All	All
Application	Ibm	Java Sdk	6.0.14.0	All	All	All
Application	Ibm	Java Sdk	6.0.15.0	All	All	All
Application	Ibm	Java Sdk	6.0.15.1	All	All	All
Application	Ibm	Java Sdk	6.0.2.0	All	All	All
Application	Ibm	Java Sdk	6.0.3.0	All	All	All
Application	Ibm	Java Sdk	6.0.4.0	All	All	All
Application	Ibm	Java Sdk	6.0.5.0	All	All	All

Application	Ibm	Java Sdk	6.0.5.0	All	All	All
Application	Ibm	Java Sdk	6.0.6.0	All	All	All
Application	Ibm	Java Sdk	6.0.7.0	All	All	All
Application	Ibm	Java Sdk	6.0.8.0	All	All	All
Application	Ibm	Java Sdk	6.0.8.1	All	All	All
Application	Ibm	Java Sdk	6.0.9.0	All	All	All
Application	Ibm	Java Sdk	6.0.9.1	All	All	All
Application	Ibm	Java Sdk	6.0.9.2	All	All	All
Application	Ibm	Java Sdk	7.0.0.0	All	All	All
Application	Ibm	Java Sdk	7.0.1.0	All	All	All
Application	Ibm	Java Sdk	7.0.2.0	All	All	All
Application	Ibm	Java Sdk	7.0.3.0	All	All	All
Application	Ibm	Java Sdk	7.0.4.0	All	All	All
Application	Ibm	Java Sdk	7.0.4.1	All	All	All
Application	Ibm	Java Sdk	7.0.4.2	All	All	All
Application	Ibm	Java Sdk	7.0.5.0	All	All	All
Application	Ibm	Java Sdk	7.0.6.0	All	All	All
Application	Ibm	Java Sdk	7.0.6.1	All	All	All
Application	Ibm	Java Sdk	7.1.0.0	All	All	All

References

Reference

Security Advisory SA59022 - IBM API Management Java Two Vulnerabilities - Secunia

About Secunia Research | Flexera

Security Bulletin: Security vulnerabilities in IBM SDK, Java™ Technology Edition (CVE-2014-0878, CVE-2014-0460, CVE-2014-0453, CVE-2014-0454)

IBM notice: The page you requested cannot be displayed

IBM X-Force Exchange

IBM Security Bulletin: IBM Operational Decision Manager, WebSphere ILOG JRules and WebSphere Business Events: Multiple security vulnerabilities

IBM Security Bulletin: Rational Insight - IBM SDK, Java Technology Edition Quarterly CPU - April 2014 (CVE-2014-0460, CVE-2014-0878) - United States

Security Bulletin: Multiple security vulnerabilities exist in the IBM SDK, Java Technology Edition provided with WebSphere eXtreme Scale

IBM Security Bulletin: Multiple vulnerabilities in current IBM SDK for Java - April 2014 CPU update for Lotus Quickr 8.5 for WebSphere Portal

Security Advisory SA59058 - IBM Lotus Expeditor Multiple Java Vulnerabilities - Secunia

IBM Security Bulletin: Two java security vulnerabilities in IBM Security Access Manager for Mobile and IBM Security Access Manager for Web

Security Advisory SA59023 - IBM Multiple Products Java Two Vulnerabilities - Secunia

IBM Security Bulletin: Multiple vulnerabilities in IBM Multi-Enterprise Integration Gateway (CVE-2014-0460, CVE-2014-0878, CVE-2014-0453)

IBM Security Bulletin: Multiple vulnerabilities in IBM API Management - United States

IBM Java SDK CVE-2014-0878 Security Bypass Vulnerability
Security Bulletin: Multiple security vulnerabilities exist in the IBM SDK, Java Technology Edition provided with WebSphere DataPower XC10 A
IBM Security Bulletin: Multiple vulnerabilities in current releases of the IBM® SDK, Java™ Technology Edition - United States
IBM Security Bulletin: AppScan Standard can be affected by vulnerability in the current IBM SDK for Java (CVE-2014-0878, CVE-2014-4244,)
Security Bulletin: Multiple vulnerabilities in the IBM SDK Java Technology Edition component of IBM MessageSight 1.0-1.1 (CVE-2014-0878,)
IBM SmartCloud Provisioning 2.1 Fix Pack 5 (SCP - 2.1.0.5) - United States
IBM Security Bulletin: Multiple security vulnerabilities in IBM SDK, Java™ Technology Edition affect IBM SmartCloud Provisioning (CVE-2014-
IBM Security Bulletin: IBM Lotus Expeditor fixes for multiple vulnerabilities in IBM JRE - United States
CVE Program record
NVD vulnerability detail
No vendor comments have been submitted for this CVE.
There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)