



CVE-2012-0744

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

Summary

CVE	CVE-2012-0744
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-08-17 20:55:00 UTC
Updated	2017-08-29 01:31:00 UTC
Description	IBM Rational ClearQuest 7.1.x through 7.1.2.7 and 8.x through 8.0.0.3 allows remote attackers to obtain potentially sensitiv



Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Rational Clearquest	7.1.1.1	All	All	All
Application	ibm	Rational Clearquest	7.1.1.2	All	All	All
Application	ibm	Rational Clearquest	7.1.1.3	All	All	All
Application	ibm	Rational Clearquest	7.1.1.4	All	All	All
Application	ibm	Rational Clearquest	7.1.1.5	All	All	All
Application	ibm	Rational Clearquest	7.1.1.6	All	All	All
Application	ibm	Rational Clearquest	7.1.1.7	All	All	All
Application	ibm	Rational Clearquest	7.1.1.8	All	All	All
Application	ibm	Rational Clearquest	7.1.2	All	All	All
Application	ibm	Rational Clearquest	7.1.2.1	All	All	All
Application	ibm	Rational Clearquest	7.1.2.2	All	All	All
Application	ibm	Rational Clearquest	7.1.2.3	All	All	All
Application	ibm	Rational Clearquest	7.1.2.4	All	All	All
Application	ibm	Rational Clearquest	7.1.2.5	All	All	All
Application	ibm	Rational Clearquest	7.1.2.6	All	All	All
Application	ibm	Rational Clearquest	8.0	All	All	All
Application	ibm	Rational Clearquest	8.0.0.1	All	All	All

Application	ibm	Rational Clearquest	8.0.0.2	All	All	All
Application	ibm	Rational Clearquest	8.0.0.3	All	All	All
Application	ibm	Rational Clearquest	7.1.1.1	All	All	All
Application	ibm	Rational Clearquest	7.1.1.2	All	All	All
Application	ibm	Rational Clearquest	7.1.1.3	All	All	All
Application	ibm	Rational Clearquest	7.1.1.4	All	All	All
Application	ibm	Rational Clearquest	7.1.1.5	All	All	All
Application	ibm	Rational Clearquest	7.1.1.6	All	All	All
Application	ibm	Rational Clearquest	7.1.1.7	All	All	All
Application	ibm	Rational Clearquest	7.1.1.8	All	All	All
Application	ibm	Rational Clearquest	7.1.2	All	All	All
Application	ibm	Rational Clearquest	7.1.2.1	All	All	All
Application	ibm	Rational Clearquest	7.1.2.2	All	All	All
Application	ibm	Rational Clearquest	7.1.2.3	All	All	All
Application	ibm	Rational Clearquest	7.1.2.4	All	All	All
Application	ibm	Rational Clearquest	7.1.2.5	All	All	All
Application	ibm	Rational Clearquest	7.1.2.6	All	All	All
Application	ibm	Rational Clearquest	8.0	All	All	All
Application	ibm	Rational Clearquest	8.0.0.1	All	All	All
Application	ibm	Rational Clearquest	8.0.0.2	All	All	All
Application	ibm	Rational Clearquest	8.0.0.3	All	All	All

References						
Reference					Source	Link
Removing the DefaultApplication template scripts from the WebSphere Application Server profile for ClearQuest Web					CONFIRM	www.ibm.com
IBM X-Force Exchange					XF	exchange.xforce.ibmcloud.com
PM66896: An information disclosure vulnerability was found					AIXAPAR	www-01.ibm.com
Security Bulletin: ClearQuest Web leftover scripts (CVE-2012-0744)					CONFIRM	www.ibm.com
CVE Program record					CVE.ORG	www.cve.org
NVD vulnerability detail					NVD	nvd.nist.gov

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](#)