



CVE-2016-9746

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

Summary

CVE	CVE-2016-9746
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-05 17:29:00 UTC
Updated	2017-07-26 01:29:00 UTC
Description	IBM Team Concert (RTC) 4.0, 5.0 and 6.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary HTML and JavaScript into the application.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Rational Collaborative Lifecycle Management	4.0.0	All	All	All
Application	ibm	Rational Collaborative Lifecycle Management	4.0.1	All	All	All
Application	ibm	Rational Collaborative Lifecycle Management	4.0.2	All	All	All
Application	ibm	Rational Collaborative Lifecycle Management	4.0.3	All	All	All
Application	ibm	Rational Collaborative Lifecycle Management	4.0.4	All	All	All
Application	ibm	Rational Collaborative Lifecycle Management	4.0.5	All	All	All
Application	ibm	Rational Collaborative Lifecycle Management	4.0.6	All	All	All
Application	ibm	Rational Collaborative Lifecycle Management	4.0.7	All	All	All
Application	ibm	Rational Collaborative Lifecycle Management	5.0	All	All	All
Application	ibm	Rational Collaborative Lifecycle Management	5.0.0	All	All	All
Application	ibm	Rational Collaborative Lifecycle Management	5.0.1	All	All	All
Application	ibm	Rational Collaborative Lifecycle Management	5.0.2	All	All	All
Application	ibm	Rational Collaborative Lifecycle Management	6.0	All	All	All
Application	ibm	Rational Collaborative Lifecycle Management	6.0.0	All	All	All
Application	ibm	Rational Collaborative Lifecycle Management	6.0.1	All	All	All
Application	ibm	Rational Collaborative Lifecycle Management	6.0.3	All	All	All
Application	ibm	Rational Collaborative Lifecycle Management	4.0.0	All	All	All

Application	lbm	Rational Collaborative Lifecycle Management	4.0.1	All	All	All
Application	lbm	Rational Collaborative Lifecycle Management	4.0.2	All	All	All
Application	lbm	Rational Collaborative Lifecycle Management	4.0.3	All	All	All
Application	lbm	Rational Collaborative Lifecycle Management	4.0.4	All	All	All
Application	lbm	Rational Collaborative Lifecycle Management	4.0.5	All	All	All
Application	lbm	Rational Collaborative Lifecycle Management	4.0.6	All	All	All
Application	lbm	Rational Collaborative Lifecycle Management	4.0.7	All	All	All
Application	lbm	Rational Collaborative Lifecycle Management	5.0	All	All	All
Application	lbm	Rational Collaborative Lifecycle Management	5.0.0	All	All	All
Application	lbm	Rational Collaborative Lifecycle Management	5.0.1	All	All	All
Application	lbm	Rational Collaborative Lifecycle Management	5.0.2	All	All	All
Application	lbm	Rational Collaborative Lifecycle Management	6.0	All	All	All
Application	lbm	Rational Collaborative Lifecycle Management	6.0.0	All	All	All
Application	lbm	Rational Collaborative Lifecycle Management	6.0.1	All	All	All
Application	lbm	Rational Collaborative Lifecycle Management	6.0.3	All	All	All
Application	lbm	Rational Team Concert	4.0	All	All	All
Application	lbm	Rational Team Concert	4.0.0	All	All	All
Application	lbm	Rational Team Concert	4.0.0.1	All	All	All
Application	lbm	Rational Team Concert	4.0.0.2	All	All	All
Application	lbm	Rational Team Concert	4.0.1	All	All	All
Application	lbm	Rational Team Concert	4.0.2	All	All	All
Application	lbm	Rational Team Concert	4.0.3	All	All	All
Application	lbm	Rational Team Concert	4.0.4	All	All	All
Application	lbm	Rational Team Concert	4.0.5	All	All	All
Application	lbm	Rational Team Concert	4.0.6	All	All	All
Application	lbm	Rational Team Concert	4.0.7	All	All	All
Application	lbm	Rational Team Concert	5.0	All	All	All
Application	lbm	Rational Team Concert	5.0.0	All	All	All
Application	lbm	Rational Team Concert	5.0.1	All	All	All
Application	lbm	Rational Team Concert	5.0.2	All	All	All
Application	lbm	Rational Team Concert	6.0	All	All	All
Application	lbm	Rational Team Concert	6.0.0	All	All	All
Application	lbm	Rational Team Concert	6.0.1	All	All	All
Application	lbm	Rational Team Concert	6.0.2	All	All	All
Application	lbm	Rational Team Concert	6.0.3	All	All	All

Application	lbn	Rational Team Concert	4.0	All	All	All
Application	lbn	Rational Team Concert	4.0.0	All	All	All
Application	lbn	Rational Team Concert	4.0.0.1	All	All	All
Application	lbn	Rational Team Concert	4.0.0.2	All	All	All
Application	lbn	Rational Team Concert	4.0.1	All	All	All
Application	lbn	Rational Team Concert	4.0.2	All	All	All
Application	lbn	Rational Team Concert	4.0.3	All	All	All
Application	lbn	Rational Team Concert	4.0.4	All	All	All
Application	lbn	Rational Team Concert	4.0.5	All	All	All
Application	lbn	Rational Team Concert	4.0.6	All	All	All
Application	lbn	Rational Team Concert	4.0.7	All	All	All
Application	lbn	Rational Team Concert	5.0	All	All	All
Application	lbn	Rational Team Concert	5.0.0	All	All	All
Application	lbn	Rational Team Concert	5.0.1	All	All	All
Application	lbn	Rational Team Concert	5.0.2	All	All	All
Application	lbn	Rational Team Concert	6.0	All	All	All
Application	lbn	Rational Team Concert	6.0.0	All	All	All
Application	lbn	Rational Team Concert	6.0.1	All	All	All
Application	lbn	Rational Team Concert	6.0.2	All	All	All
Application	lbn	Rational Team Concert	6.0.3	All	All	All

References

Reference	Source
Malformed Request	BID
IBM Rational Team Concert Multiple Input Validation Flaws Let Remote Users Conduct Cross-Site Scripting Attacks - SecurityTracker	SEC7
IBM X-Force Exchange	MISC
Security Bulletin: Cross-site scripting vulnerabilities affect IBM® Rational® Team Concert	CONI
CVE Program record	CVE.
NVD vulnerability detail	NVD



No vendor comments have been submitted for this CVE.

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

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