



CVE-2021-20519

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

Summary

CVE	CVE-2021-20519
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-12 18:15:00 UTC
Updated	2021-04-13 19:56:00 UTC
Description	IBM Jazz Team Server products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code into the page. This can be used to steal sensitive information, such as cookies, and to perform actions on behalf of the user. The vulnerability is present in IBM Jazz Team Server products, including IBM Jazz Team Server, IBM Jazz Team Server for SAP, and IBM Jazz Team Server for SAP NetWeaver. The vulnerability is present in IBM Jazz Team Server products, including IBM Jazz Team Server, IBM Jazz Team Server for SAP, and IBM Jazz Team Server for SAP NetWeaver. The vulnerability is present in IBM Jazz Team Server products, including IBM Jazz Team Server, IBM Jazz Team Server for SAP, and IBM Jazz Team Server for SAP NetWeaver.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Collaborative Lifecycle Management	6.0.2	All	All	All
Application	ibm	Collaborative Lifecycle Management	6.0.6	All	All	All
Application	ibm	Collaborative Lifecycle Management	6.0.6.1	All	All	All
Application	ibm	Doors Next	7.0.0	All	All	All
Application	ibm	Doors Next	7.0.1	All	All	All
Application	ibm	Doors Next	7.0.2	All	All	All
Application	ibm	Engineering Insights	7.0.0	All	All	All
Application	ibm	Engineering Insights	7.0.1	All	All	All
Application	ibm	Engineering Insights	7.0.2	All	All	All
Application	ibm	Engineering Lifecycle Management	7.0.0	All	All	All
Application	ibm	Engineering Lifecycle Management	7.0.1	All	All	All
Application	ibm	Engineering Lifecycle Management	7.0.2	All	All	All
Application	ibm	Engineering Requirements Management Doors Next	6.0.2	All	All	All
Application	ibm	Engineering Requirements Management Doors Next	6.0.6	All	All	All
Application	ibm	Engineering Requirements Management Doors Next	6.0.6.1	All	All	All
Application	ibm	Engineering Test Management	7.0.0	All	All	All
Application	ibm	Engineering Test Management	7.0.1	All	All	All

Application	lbn	Engineering Test Management	7.0.2	All	All	All
Application	lbn	Engineering Workflow Management	7.0.0	All	All	All
Application	lbn	Engineering Workflow Management	7.0.1	All	All	All
Application	lbn	Engineering Workflow Management	7.0.2	All	All	All
Application	lbn	Rational Engineering Lifecycle Manager	6.0.2	All	All	All
Application	lbn	Rational Engineering Lifecycle Manager	6.0.6	All	All	All
Application	lbn	Rational Engineering Lifecycle Manager	6.0.6.1	All	All	All
Application	lbn	Rational Quality Manager	6.0.2	All	All	All
Application	lbn	Rational Quality Manager	6.0.6	All	All	All
Application	lbn	Rational Quality Manager	6.0.6.1	All	All	All
Application	lbn	Rational Team Concert	6.0.2	All	All	All
Application	lbn	Rational Team Concert	6.0.6	All	All	All
Application	lbn	Rational Team Concert	6.0.6.1	All	All	All
Application	lbn	Removable Media Management	6.0.2	All	All	All
Application	lbn	Removable Media Management	6.0.6	All	All	All
Application	lbn	Removable Media Management	6.0.6.1	All	All	All
Application	lbn	Removable Media Management	7.0.0	All	All	All
Application	lbn	Removable Media Management	7.0.1	All	All	All
Application	lbn	Rhapsody Model Manager	6.0.2	All	All	All
Application	lbn	Rhapsody Model Manager	6.0.6	All	All	All
Application	lbn	Rhapsody Model Manager	6.0.6.1	All	All	All

References

Reference	Source	Link
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
Security Bulletin: Multiple vulnerabilities affect IBM Jazz Foundation and IBM Engineering products.	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.

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