CVE-2017-1653

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-1653
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-26 21:29:00 UTC
Updated	2018-02-09 20:06:00 UTC
Description	IBM Jazz Foundation (IBM Rational Collaborative Lifecycle Management 6.0.x) is vulnerable to cross-site scripting. This vul

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	All	All	All	All
Application	Ibm	Rational Doors Next Generation	All	All	All	All
Application	Ibm	Rational Engineering Lifecycle Manager	All	All	All	All
Application	Ibm	Rational Quality Manager	All	All	All	All
Application	Ibm	Rational Rhapsody Design Manager	All	All	All	All
Application	Ibm	Rational Software Architect Design Manager	6.0	All	All	All
Application	Ibm	Rational Software Architect Design Manager	6.0.1	All	All	All
Application	Ibm	Rational Software Architect Design Manager	6.0	All	All	All
Application	Ibm	Rational Software Architect Design Manager	6.0.1	All	All	All
Application	Ibm	Rational Team Concert	All	All	All	All

References

Reference
Security Bulletin: Cross-site scripting vulnerability in IBM Jazz Team Server affect IBM Rational products based on IBM Jazz technology
IBM X-Force Exchange
Multiple IBM Products CVE-2017-1653 Cross Site Scripting Vulnerability
IBM Rational Team Concert Input Validation Flaw in Jazz Foundation Lets Remote Users Conduct Cross-Site Scripting Attacks - SecurityTrac

IBM Rational Software Architect Input Validation Flaw in Jazz Foundation Lets Remote Users Conduct Cross-Site Scripting Attacks - SecurityT
IBM Rational Quality Manager Input Validation Flaw in Jazz Foundation Lets Remote Users Conduct Cross-Site Scripting Attacks - SecurityTr
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**