



# CVE-2018-1952

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

## Summary

<b>CVE</b>	CVE-2018-1952
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@us.ibm.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-03-14 22:29:00 UTC
<b>Updated</b>	2019-10-09 23:39:00 UTC
<b>Description</b>	IBM Jazz Foundation (IBM Rational Engineering Lifecycle Manager 5.0 through 6.0.6) is vulnerable to cross-site scripting. 7

## 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	All	All	All	All
Application	ibm	Rational Team Concert	All	All	All	All

## References

Reference	Source	Link
Multiple IBM Rational Products Cross Site Scripting and HTTP Header Injection Vulnerabilities	BID	<a href="http://www.securityfocus.com/bid/104848">www.securityfocus.com/bid/104848</a>
Security Bulletin: Security vulnerabilities affect multiple IBM Rational products based on IBM Jazz technology	CONFIRM	<a href="http://www.ibm.com/support/ctgsec/docmgr.jsp?aid=ibmcom-01547">www.ibm.com/support/ctgsec/docmgr.jsp?aid=ibmcom-01547</a>
IBM X-Force Exchange	XF	<a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/104848">exchange.xforce.ibmcloud.com/vulnerabilities/104848</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org/CVE/nvd/cve/2018/1952">www.cve.org/CVE/nvd/cve/2018/1952</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov/vuln/detail/CVE-2018-1952">nvd.nist.gov/vuln/detail/CVE-2018-1952</a>

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](#)