



CVE-2017-1127

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2017-1127
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-08 19:59:00 UTC
Updated	2017-02-15 13:14:00 UTC
Description	IBM Rational DOORS Next Generation 4.0, 5.0 and 6.0 is vulnerable to cross-site scripting. This vulnerability allows users t

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Rational Doors Next Generation	5.0	All	All	All
Application	ibm	Rational Doors Next Generation	5.0.0	All	All	All
Application	ibm	Rational Doors Next Generation	5.0.1	All	All	All
Application	ibm	Rational Doors Next Generation	5.0.2	All	All	All
Application	ibm	Rational Doors Next Generation	6.0	All	All	All
Application	ibm	Rational Doors Next Generation	6.0.0	All	All	All
Application	ibm	Rational Doors Next Generation	6.0.1	All	All	All
Application	ibm	Rational Doors Next Generation	6.0.2	All	All	All
Application	ibm	Rational Doors Next Generation	5.0	All	All	All
Application	ibm	Rational Doors Next Generation	5.0.0	All	All	All
Application	ibm	Rational Doors Next Generation	5.0.1	All	All	All
Application	ibm	Rational Doors Next Generation	5.0.2	All	All	All
Application	ibm	Rational Doors Next Generation	6.0	All	All	All
Application	ibm	Rational Doors Next Generation	6.0.0	All	All	All
Application	ibm	Rational Doors Next Generation	6.0.1	All	All	All
Application	ibm	Rational Doors Next Generation	6.0.2	All	All	All
Application	ibm	Rational Requirements Composer	4.0	All	All	All

Application	ibm	Rational Requirements Composer	4.0.0	All	All	All
Application	ibm	Rational Requirements Composer	4.0.0.1	All	All	All
Application	ibm	Rational Requirements Composer	4.0.0.2	All	All	All
Application	ibm	Rational Requirements Composer	4.0.1	All	All	All
Application	ibm	Rational Requirements Composer	4.0.2	All	All	All
Application	ibm	Rational Requirements Composer	4.0.3	All	All	All
Application	ibm	Rational Requirements Composer	4.0.4	All	All	All
Application	ibm	Rational Requirements Composer	4.0.5	All	All	All
Application	ibm	Rational Requirements Composer	4.0.6	All	All	All
Application	ibm	Rational Requirements Composer	4.0.7	All	All	All
Application	ibm	Rational Requirements Composer	4.0	All	All	All
Application	ibm	Rational Requirements Composer	4.0.0	All	All	All
Application	ibm	Rational Requirements Composer	4.0.0.1	All	All	All
Application	ibm	Rational Requirements Composer	4.0.0.2	All	All	All
Application	ibm	Rational Requirements Composer	4.0.1	All	All	All
Application	ibm	Rational Requirements Composer	4.0.2	All	All	All
Application	ibm	Rational Requirements Composer	4.0.3	All	All	All
Application	ibm	Rational Requirements Composer	4.0.4	All	All	All
Application	ibm	Rational Requirements Composer	4.0.5	All	All	All
Application	ibm	Rational Requirements Composer	4.0.6	All	All	All
Application	ibm	Rational Requirements Composer	4.0.7	All	All	All

References

Reference

[IBM Security Bulletin: Vulnerability in Rational DOORS Next Generation with potential for Cross-Site Scripting attack \(CVE-2017-1127, CVE-2017-1128\)](#)

[Multiple IBM Products CVE-2017-1127 Cross Site Scripting Vulnerability](#)

[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.

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