



# CVE-2017-1128

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2017-1128
<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>	2017-02-08 19:59:00 UTC
<b>Updated</b>	2017-02-15 14:09:00 UTC
<b>Description</b>	IBM Rational DOORS Next Generation 4.0, 5.0, and 6.0 is vulnerable to cross-site scripting. This vulnerability allows users

## 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	6.0.0	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	6.0.0	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	<a href="#">Rational Requirements Composer</a>	4.0.0.2	All	All	All
Application	ibm	<a href="#">Rational Requirements Composer</a>	4.0.1	All	All	All
Application	ibm	<a href="#">Rational Requirements Composer</a>	4.0.2	All	All	All
Application	ibm	<a href="#">Rational Requirements Composer</a>	4.0.3	All	All	All
Application	ibm	<a href="#">Rational Requirements Composer</a>	4.0.4	All	All	All
Application	ibm	<a href="#">Rational Requirements Composer</a>	4.0.5	All	All	All
Application	ibm	<a href="#">Rational Requirements Composer</a>	4.0.6	All	All	All
Application	ibm	<a href="#">Rational Requirements Composer</a>	4.0.7	All	All	All
Application	ibm	<a href="#">Rational Requirements Composer</a>	4.0	All	All	All
Application	ibm	<a href="#">Rational Requirements Composer</a>	4.0.0	All	All	All
Application	ibm	<a href="#">Rational Requirements Composer</a>	4.0.0.1	All	All	All
Application	ibm	<a href="#">Rational Requirements Composer</a>	4.0.0.2	All	All	All
Application	ibm	<a href="#">Rational Requirements Composer</a>	4.0.1	All	All	All
Application	ibm	<a href="#">Rational Requirements Composer</a>	4.0.2	All	All	All
Application	ibm	<a href="#">Rational Requirements Composer</a>	4.0.3	All	All	All
Application	ibm	<a href="#">Rational Requirements Composer</a>	4.0.4	All	All	All
Application	ibm	<a href="#">Rational Requirements Composer</a>	4.0.5	All	All	All
Application	ibm	<a href="#">Rational Requirements Composer</a>	4.0.6	All	All	All
Application	ibm	<a href="#">Rational Requirements Composer</a>	4.0.7	All	All	All

## References

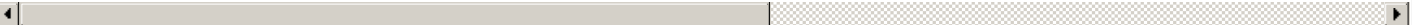
### Reference

IBM Security Bulletin: Vulnerability in Rational DOORS Next Generation with potential for Cross-Site Scripting attack (CVE-2017-1127, CVE-2

Multiple IBM Products CVE-2017-1128 Unspecified 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.

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)