



CVE-2018-1731

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

Summary

CVE	CVE-2018-1731
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-04-03 14:29:00 UTC
Updated	2019-04-05 07:29:00 UTC
Description	IBM DOORS Next Generation (DNG/RRC) 5.0 through 5.0.3 and 6.0 through 6.0.6 is vulnerable to cross-site scripting. This

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Doors Next Generation	All	All	All	All
Application	ibm	Doors Next Generation	All	All	All	All

References

Reference	Source	Link
IBM Rational DOORS Next Generation Multiple Cross Site Scripting Vulnerabilities	BID	www.securityfocus.com/bid/104841
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com/entries/104841
Security Bulletin: Vulnerabilities in Rational DOORS Next Generation with potential for cross-site scripting attack	CONFIRM	www.ibm.com/support/techdocs/wwsidx.jsp?wws_content_base=/en_US/SECURITY_BULLETINS/2019040301
CVE Program record	CVE.ORG	www.cve.org/CVE/nvd/cve/2018/1731
NVD vulnerability detail	NVD	nvd.nist.gov/vuln/detail/CVE-2018-1731

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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