

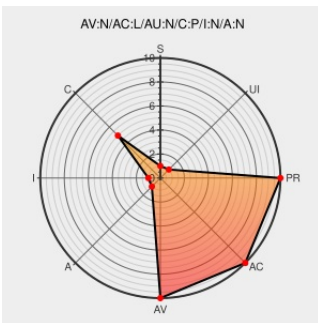


CVE-2010-4600

Published on: 12/29/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:00 PM UTC

CVE-2010-4600

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Dojo Toolkit](#) from [Dojofoundation](#) contain the following vulnerability:

Dojo Toolkit, as used in the Web client in IBM Rational ClearQuest 7.1.1.x before 7.1.1.4 and 7.1.2.x before 7.1.2.1, allows remote attackers to read cookies by navigating to a Dojo file, related to an "open direct" issue.

CVE-2010-4600 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

[public.dhe.ibm.com](#)
[text/plain](#)

CONFIRM
public.dhe.ibm.com/software/rational/clearquest/7.1.1/7.1.1.4-RATL-RCQ/7.1.1.4-RATL-RCQ.ux.readme

IBM PM15146: CQ Vulnerability: cookies shown browsing to dojo file aka 'open direct' - United States

[www-01.ibm.com](#)
[text/html](#)

AIXAPAR PM15146

IBM Rational ClearQuest Multiple Vulnerabilities - Advisories - Community

[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)

SECUNIA 42624

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dojofoundation	Dojo Toolkit	All	All	All	All
Application	Dojofoundation	Dojo Toolkit	All	All	All	All
Application	ibm	Rational Clearquest	7.1.1.1	All	All	All
Application	ibm	Rational Clearquest	7.1.1.2	All	All	All
Application	ibm	Rational Clearquest	7.1.1.3	All	All	All
Application	ibm	Rational Clearquest	7.1.2	All	All	All
Application	ibm	Rational Clearquest	7.1.1.1	All	All	All
Application	ibm	Rational Clearquest	7.1.1.2	All	All	All
Application	ibm	Rational Clearquest	7.1.1.3	All	All	All
Application	ibm	Rational Clearquest	7.1.2	All	All	All
cpe:2.3:a:dojofoundation:dojo_toolkit:*.***.***.***:						
cpe:2.3:a:dojofoundation:dojo_toolkit:*.***.***.***:						
cpe:2.3:a:ibm:rational_clearquest:7.1.1.1:*.***.***.***:						
cpe:2.3:a:ibm:rational_clearquest:7.1.1.2:*.***.***.***:						
cpe:2.3:a:ibm:rational_clearquest:7.1.1.3:*.***.***.***:						
cpe:2.3:a:ibm:rational_clearquest:7.1.2:*.***.***.***:						
cpe:2.3:a:ibm:rational_clearquest:7.1.1.1:*.***.***.***:						
cpe:2.3:a:ibm:rational_clearquest:7.1.1.2:*.***.***.***:						
cpe:2.3:a:ibm:rational_clearquest:7.1.1.3:*.***.***.***:						
cpe:2.3:a:ibm:rational_clearquest:7.1.2:*.***.***.***:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)