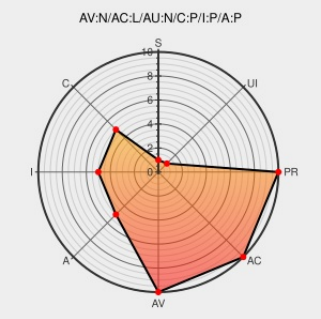
CVE-2012-4816

Published on: 12/26/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:14 PM UTC

CVE-2012-4816

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Rational Automation Framework from Ibm contain the following vulnerability:

IBM Rational Automation Framework (RAF) 3.x through 3.0.0.5 allows remote attackers to bypass intended Env Gen Wizard (aka Environment Generation Wizard) access restrictions by visiting context roots in HTTP sessions on port 8080.

CVE-2012-4816 has been assigned by psirt@us.ibm.com to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Security Bulletin: Rational Automation Framework Environment Wizard Vulnerability (CVE-2012-4816)	Vendor Advisory, www-01.ibm.com, text/html	CONFIRM www-01.ibm.com/support/docview.wss?uid=swg21620359
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF raf-environmentwizard-security-bypass(78379)

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Rational Automation Framework	3.0	All	All	All
Application	Ibm	Rational Automation Framework	3.0.0.1	All	All	All
Application	Ibm	Rational Automation Framework	3.0.0.2	All	All	All
Application	Ibm	Rational Automation Framework	3.0.0.3	All	All	All
Application	Ibm	Rational Automation Framework	3.0.0.4	All	All	All
Application	Ibm	Rational Automation Framework	3.0.0.5	All	All	All
Application	Ibm	Rational Automation Framework	3.0	All	All	All
Application	Ibm	Rational Automation Framework	3.0.0.1	All	All	All
Application	Ibm	Rational Automation Framework	3.0.0.2	All	All	All
Application	Ibm	Rational Automation Framework	3.0.0.3	All	All	All
Application	Ibm	Rational Automation Framework	3.0.0.4	All	All	All
Application	Ibm	Rational Automation Framework	3.0.0.5	All	All	All

cpe:2.3:a:ibm:rational_automation_framework:3.0:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:rational_automation_framework:3.0.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:rational_automation_framework:3.0.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:rational_automation_framework:3.0.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:rational_automation_framework:3.0.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:rational_automation_framework:3.0.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:rational_automation_framework:3.0:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:rational_automation_framework:3.0.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:rational_automation_framework:3.0.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:rational_automation_framework:3.0.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:rational_automation_framework:3.0.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:rational_automation_framework:3.0.0.5:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report