



CVE-2011-1034

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

Summary

CVE	CVE-2011-1034
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-02-16 03:00:00 UTC
Updated	2011-02-16 05:00:00 UTC
Description	Cross-site scripting (XSS) vulnerability in the UI in IBM Rational Build Forge 7.0.2 allows remote attackers to inject arbitrary

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Rational Build Forge	7.0.2	All	All	All
Application	ibm	Rational Build Forge	7.0.2	All	All	All

References

Reference	Source	Link
IBM Rational Build Forge Cross-Site Scripting Vulnerability - Secunia.com	SECUNIA	secu
IBM Rational Build Forge 'fullcontrol/' Cross Site Scripting Vulnerability	BID	www.
PM05187: Build Forge UI has cross site scripting vulnerability.	AIXAPAR	www.
IBM Rational Build Forge Input Validation Flaw in User Interface Permits Cross-Site Scripting Attacks - SecurityTracker	SECTRACK	secu
70763	OSVDB	www.
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.n

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)