



CVE-2007-6617

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

Summary

CVE	CVE-2007-6617
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-01-03 23:46:00 UTC
Updated	2008-11-15 07:05:00 UTC
Description	Cross-site scripting (XSS) vulnerability in 500page.jsp in JIRA Enterprise Edition before 3.12.1 allows remote attackers to ir

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atlassian	Jira	All	All	enterprise	All

References

Reference	Source	Link
JIRA Security Advisory 2007-12-24 - JIRA - Confluence	CONFIRM	confluence.atlassian.com
Atlassian JIRA '500page.jsp' Cross-Site Scripting Vulnerability	BID	www.securityfocus.com
[#CONF-9560] Cross-site scripting vulnerability in 500page.jsp - Atlassian JIRA	CONFIRM	jira.atlassian.com
Atlassian JIRA Enterprise Edition Cross-Site Scripting and Security Bypass - Advisories - Secunia	SECUNIA	secunia.com
42768	OSVDB	osvdb.org
Atlassian JIRA Multiple Security Bypass Weaknesses	BID	www.securityfocus.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)