



CVE-2008-6423

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

Summary

CVE	CVE-2008-6423
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-03-06 18:30:00 UTC
Updated	2017-09-29 01:33:00 UTC
Description	Directory traversal vulnerability in passwiki.php in PassWiki 0.9.16 RC3 and earlier allows remote attackers to read arbitrary

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	I-apps	Passwiki	0.9.10	All	All	All
Application	I-apps	Passwiki	0.9.11	All	All	All
Application	I-apps	Passwiki	0.9.12	All	All	All
Application	I-apps	Passwiki	0.9.13	All	All	All
Application	I-apps	Passwiki	0.9.14	All	All	All
Application	I-apps	Passwiki	0.9.15	All	All	All
Application	I-apps	Passwiki	0.9.15	beta	All	All
Application	I-apps	Passwiki	0.9.15	beta2	All	All
Application	I-apps	Passwiki	0.9.15	rc1	All	All
Application	I-apps	Passwiki	0.9.16	beta1	All	All
Application	I-apps	Passwiki	0.9.16	beta2	All	All
Application	I-apps	Passwiki	0.9.16	beta3	All	All
Application	I-apps	Passwiki	0.9.16	rc1	All	All
Application	I-apps	Passwiki	0.9.16	rc2	All	All
Application	I-apps	Passwiki	0.9.3	All	All	All
Application	I-apps	Passwiki	0.9.5	All	All	All
Application	I-apps	Passwiki	0.9.6	All	All	All

Application	I-apps	Passwiki	0.9.7	All	All	All
Application	I-apps	Passwiki	0.9.8	All	All	All
Application	I-apps	Passwiki	0.9.9	All	All	All
Application	I-apps	Passwiki	All	rc3	All	All
Application	I-apps	Passwiki	0.9.10	All	All	All
Application	I-apps	Passwiki	0.9.11	All	All	All
Application	I-apps	Passwiki	0.9.12	All	All	All
Application	I-apps	Passwiki	0.9.13	All	All	All
Application	I-apps	Passwiki	0.9.14	All	All	All
Application	I-apps	Passwiki	0.9.15	All	All	All
Application	I-apps	Passwiki	0.9.15	beta	All	All
Application	I-apps	Passwiki	0.9.15	beta2	All	All
Application	I-apps	Passwiki	0.9.15	rc1	All	All
Application	I-apps	Passwiki	0.9.16	beta1	All	All
Application	I-apps	Passwiki	0.9.16	beta2	All	All
Application	I-apps	Passwiki	0.9.16	beta3	All	All
Application	I-apps	Passwiki	0.9.16	rc1	All	All
Application	I-apps	Passwiki	0.9.16	rc2	All	All
Application	I-apps	Passwiki	0.9.3	All	All	All
Application	I-apps	Passwiki	0.9.5	All	All	All
Application	I-apps	Passwiki	0.9.6	All	All	All
Application	I-apps	Passwiki	0.9.7	All	All	All
Application	I-apps	Passwiki	0.9.8	All	All	All
Application	I-apps	Passwiki	0.9.9	All	All	All

References						
Reference				Source	Link	
45853				OSVDB	osvdb.org	
Security Advisory SA30496 - PassWiki 'site_id' Local File Inclusion Vulnerability - Secunia				SECUNIA	secunia.com	
PassWiki 0.9.16 RC3 - 'site_id' Local File Inclusion - PHP webapps Exploit				EXPLOIT-DB	www.exploit-db.com	
IBM X-Force Exchange				XF	exchange.xforce.ibm	
PassWiki 'site_id' Parameter Local File Include Vulnerability				BID	www.securityfocus.c	
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](#)