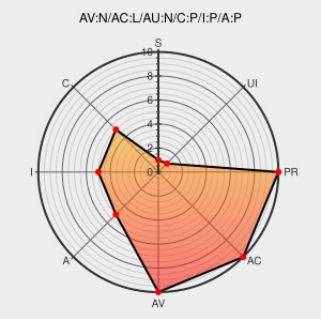
CVE-2005-1925

Published on: 11/18/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:24 PM UTC

CVE-2005-1925

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



Certain versions of Tikiwiki Cms/groupware from Tiki contain the following vulnerability:

Multiple directory traversal vulnerabilities in Tikiwiki before 1.9.1 allow remote attackers to read arbitrary files and execute commands via (1) the suck_url parameter to tiki-editpage.php or (2) language parameter to tiki-user_preferences.php.

CVE-2005-1925 has been assigned by cve@mitre.org 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
iDefense Security Intelligence Services - Information Security Services - Verisign	Patch, Vendor Advisory, www.idefense.com, text/xml	IDEFENSE 20051110 Tikiwiki tiki-editpage Arbitrary File Exposure Vulnerability
TikiWiki Tiki-User_Preferences.PHP Directory Traversal Vulnerability	cve.report (archive), text/html	BID 15392
TikiWiki Tiki-Editpage.PHP Directory Traversal Vulnerability	cve.report (archive), text/html	BID 15390
SecurityTracker.com Archives - TikiWiki Input Validation Holes in 'user_preferences.php' and 'editpage.php' Let Remote Users Execute Arbitrary Code	securitytracker.com, text/html	SECTRACK 1015190
iDefense Security Intelligence Services - Information Security Services - Verisign	Patch, Vendor Advisory	IDEFENSE 20051110 Tikiwiki tiki-user_preferences

	www.idefense.com text/xml	Command Injection Vulnerability
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF tikiwiki-tikiuserpreferences-dir-traversal(23099)
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF tikiwiki-tikieditpage-directory-traversal(23095)

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tiki	Tikiwiki Cms/groupware	1.6.1	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.0	rc1	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.0	rc2	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.0	rc3	All	All
Application	Tiki	Tikiwiki Cms/groupware	All	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.6.1	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.0	rc1	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.0	rc2	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.0	rc3	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.6.1	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.0	rc1	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.0	rc2	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.0	rc3	All	All
Application	Tiki	Tikiwiki Cms/groupware	All	All	All	All

cpe:2.3:a:tiki:tikiwiki_cms/groupware:1.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:tiki:tikiwiki_cms/groupware:1.9.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:tiki:tikiwiki_cms/groupware:1.9.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:tiki:tikiwiki_cms/groupware:1.9.0:rc3:*:*:*:*:*:*:

cpe:2.3:a:tiki:tikiwiki_cms/groupware:*:*:*:*:*:*:*:*:

cpe:2.3:a:tiki:tikiwiki_cms\/groupware:1.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:tiki:tikiwiki_cms\/groupware:1.9.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:tiki:tikiwiki_cms\/groupware:1.9.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:tiki:tikiwiki_cms\/groupware:1.9.0:rc3:*:*:*:*:*:*:

cpe:2.3:a:tiki:tikiwiki_cms\/groupware:1.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:tiki:tikiwiki_cms\/groupware:1.9.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:tiki:tikiwiki_cms\/groupware:1.9.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:tiki:tikiwiki_cms\/groupware:1.9.0:rc3:*:*:*:*:*:*:

cpe:2.3:a:tiki:tikiwiki_cms\/groupware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→