



CVE-2005-3528

Published on: 11/20/2005 12:00:00 AM UTC

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

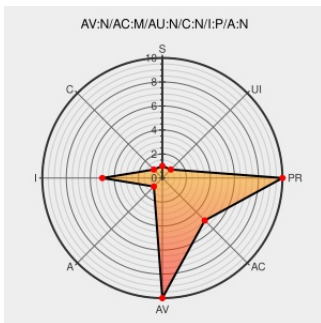
CVE-2005-3528

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Tikiwiki Cms/groupware](#) from [Tiki](#) contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in tiki-view_forum_thread.php in TikiWiki 1.9.0 through 1.9.2 allows remote attackers to inject arbitrary web script or HTML via the topics_offset parameter.

CVE-2005-3528 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

PARTIAL

NONE

CVE References

Description

Tags

Link

TikiWiki Tiki-view_forum_thread.PHP Cross-Site Scripting Vulnerability

[Exploit](#)
[cve.report \(archive\)](#)
[text/html](#)

[🌐](#) [BID 15371](#)

SecurityFocus

[www.securityfocus.com](#)
[text/html](#)

[🌐](#) [BUGTRAQ 20051109 Multiple security issues in TikiWiki 1.9.x](#)

TikiWiki "topics_offset" Cross-Site Scripting Vulnerability - Advisories - Secunia

[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)

[✖](#) [SECUNIA 17521](#)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[www.vupen.com](#)
[text/html](#)

[🌐](#) [VUPEN ADV-2005-2376](#)

Error 403 - Forbidden

[Exploit](#)
[Vendor Advisory](#)
[moritz-naumann.com](#)

[🌐](#) [MISC moritz-naumann.com/adv/0003/tikiw/0003.txt](#)

[text/plain](#)[Inactive Link](#)[Not Archived](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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	1.9.0	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.1	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.2	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.0	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.1	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.2	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.0	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.1	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.2	All	All	All
cpe:2.3:a:tiki:tikiwiki_cms/groupware:1.9.0:*:*:*:*:*:						
cpe:2.3:a:tiki:tikiwiki_cms/groupware:1.9.1:*:*:*:*:*:						
cpe:2.3:a:tiki:tikiwiki_cms/groupware:1.9.2:*:*:*:*:*:						
cpe:2.3:a:tiki:tikiwiki_cms\groupware:1.9.0:*:*:*:*:*:						
cpe:2.3:a:tiki:tikiwiki_cms\groupware:1.9.1:*:*:*:*:*:						
cpe:2.3:a:tiki:tikiwiki_cms\groupware:1.9.2:*:*:*:*:*:						
cpe:2.3:a:tiki:tikiwiki_cms\groupware:1.9.0:*:*:*:*:*:						
cpe:2.3:a:tiki:tikiwiki_cms\groupware:1.9.1:*:*:*:*:*:						
cpe:2.3:a:tiki:tikiwiki_cms\groupware:1.9.2:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)[Next ID →](#)

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)