



CVE-2008-3654

Published on: 08/12/2008 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:12 PM UTC

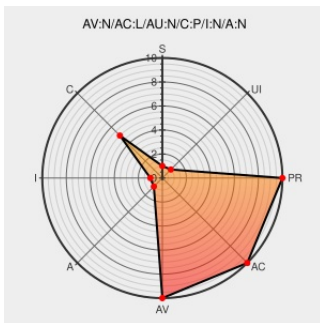
CVE-2008-3654

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Unspecified vulnerability in TikiWiki CMS/Groupware before 2.0 allows attackers to obtain "path and PHP configuration" via unknown vectors.

CVE-2008-3654 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access Vector

NETWORK

Access Complexity

LOW

Authentication

NONE

Confidentiality Impact

PARTIAL

Integrity Impact

NONE

Availability Impact

NONE

CVE References

Description

Tags

Link

info.tw.o - Welcome to TikiWiki CMS/Groupware : TikiWiki CMS/Groupware 2.0 is released!

[web.archive.org](#)

[text/html](#)

[Inactive Link](#)

[Not Archived](#)

[CONFIRM info.tikiwiki.org/tiki-read_article.php?articleId=35](#)

tw.o : TikiWiki CMS/Groupware : ReleaseNotes20

[tikiwiki.org](#)

[text/xml](#)

[CONFIRM tikiwiki.org/ReleaseNotes20](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)

[text/html](#)

[XF tikiwikicms-unspecified-path-disclosure\(44421\)](#)

By selecting these links, you may be leaving CVEreport workspace. 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	1.6.1	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.0	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	1.9.1	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.2	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.3	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.4	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.5	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.6	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.7	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.8	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.8.1	All	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	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	1.9.1	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.2	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.3	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.4	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.5	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.6	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.7	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.8	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.8.1	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.6.1	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.0	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	1.9.1	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.2	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.3	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.4	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.5	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.6	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.7	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.8	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	1.9.8.1	All	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:****:****:						
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:1.9.1:****:****:						
cpe:2.3:a:tiki:tikiwiki_cms/groupware:1.9.2:****:****:						
cpe:2.3:a:tiki:tikiwiki_cms/groupware:1.9.3:****:****:						
cpe:2.3:a:tiki:tikiwiki_cms/groupware:1.9.4:****:****:						
cpe:2.3:a:tiki:tikiwiki_cms/groupware:1.9.5:****:****:						
cpe:2.3:a:tiki:tikiwiki_cms/groupware:1.9.6:****:****:						
cpe:2.3:a:tiki:tikiwiki_cms/groupware:1.9.7:****:****:						
cpe:2.3:a:tiki:tikiwiki_cms/groupware:1.9.8:****:****:						
cpe:2.3:a:tiki:tikiwiki_cms/groupware:1.9.8.1:****:****:						
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:****:****:						
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:1.9.1:::*:*:*:*:
```

```
cpe:2.3:a:tiki:tikiwiki_cms\groupware:1.9.2:*:*:*:*:*:*:
```

cpe:2.3:a:tiki:tikiwiki_cms\groupware:1.9.3.*:*:*:*:*:*:

```
cpe:2.3:a:tiki:tikiwiki_cms\groupware:1.9.4.*:*:*:*:*:*:
```

```
cpe:2.3:a:tiki:tikiwiki_cms\groupware:1.9.5:*:*:*:*:*:*:
```

cpe:2.3:a:tiki:tikiwiki_cms\groupware:1.9.6:*:*:*:*:*:

```
cpe:2.3:a:tiki:tikiwiki_cms\groupware:1.9.7:*:*:*:*:*.*
```

```
cpe:2.3:a:tiki:tikiwiki_cms\groupware:1.9.8.*:*:*:*:*:*
```

```
cpe:2.3:a:tiki:tikiwiki_cms\groupware:1.9.8.1:*:*:*:*:*.*
```

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

```
cpe:2.3:a:tiki:tikiwiki_cms\groupware:1.9.0:*:*:*:*:*:*
```

```
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:1.9.1:*:*:*:*:*:*
```

```
cpe:2.3:a:tiki:tikiwiki_cms\groupware:1.9.2:*:*:*:*:*:*
```

```
cpe:2.3:a:tiki:tikiwiki_cms\groupware:1.9.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:tiki:tikiwiki_cms\groupware:1.9.4:*:*:*:*:*:
```

```
cpe:2.3:a:tiki:tikiwiki cms\groupware:1.9.5:*.:.:*.:.:*.:.:*
```

```
cpe:2.3:a:tiki:tikiwiki_cms\groupware:1.9.6:::*:*:*.*
```

```
cpe:2.3:a:tiki:tikiwiki_cms\groupware:1.9.7:::*:*:*.*
```

```
cpe:2.3:a:tiki:tikiwiki_cms\groupware:1.9.8:*:*:*:*:*:
```

```
cpe:2.3:a:tiki:tikiwiki cms\groupware:1.9.8.1:*:*:*:*:*:*
```

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

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023  |

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](#).

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