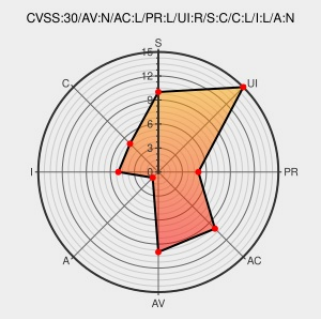
CVE-2018-7188

Published on: 02/16/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:37 PM UTC

CVE-2018-7188

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



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

An XSS vulnerability (via an SVG image) in Tiki before 18 allows an authenticated user to gain administrator privileges if an administrator opens a wiki page with a malicious SVG image, related to lib/filegals/filegallib.php.

CVE-2018-7188 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.4 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
oss-security - XSS vulnerability in Tiki < 18	Mailing List Third Party Advisory openwall.com text/html	MISC openwall.com/lists/oss-security/2018/02/16/1

Tiki Wiki CMS Groupware / SVN-Code / Commit [r65327]	Patch sourceforge.net text/html	MISC sourceforge.net/p/tikiwiki/code/65327

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	All	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	All	All	All	All
Application	Tiki	Tikiwiki Cms/groupware	All	All	All	All

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→