



CVE-2022-29351

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

Summary

CVE	CVE-2022-29351
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-16 14:15:00 UTC
Updated	2022-05-24 17:21:00 UTC
Description	An arbitrary file upload vulnerability in the file upload module of Tiddlywiki5 v5.2.2 allows attackers to execute arbitrary code

Risk And Classification

Problem Types: CWE-434

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tiddlywiki	Tiddlywiki5	5.2.2	All	All	All

References

Reference	Source	Link
tiddlywiki5.com	MISC	tiddlywiki5.com
GitHub - jimcola99/corruptsvgfile: Corrupt SVG File With XSS	MISC	github.com
GitHub - Jermolene/TiddlyWiki5: A self-contained JavaScript wiki for the browser, Node.js, AWS Lambda etc.	MISC	github.com
TiddlyWiki5 SVG Attack - YouTube	MISC	www.youtube.co
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.

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