



CVE-2023-36809

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

Summary

CVE	CVE-2023-36809
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-05 22:15:00 UTC
Updated	2023-07-12 17:38:00 UTC
Description	Kiwi TCMS, an open source test management system allows users to upload attachments to test plans, test cases, etc. Ver

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kiwitcms	Kiwi Tcms	All	All	All	All

References

Reference	Source	Link	Tags
huntr – Security Bounties for any GitHub repository	MISC	huntr.dev	
Better enforcing of mime type for uploads · kiwitcms/Kiwi@ffb0045 · GitHub	MISC	www.github.com	
Misconfigured HTTP headers allowing stored XSS execution · Advisory · kiwitcms/Kiwi · GitHub	MISC	github.com	
Kiwi TCMS - Kiwi TCMS 12.5	MISC	kiwitcms.org	
Sanitize test plan name in tree_view_html() · kiwitcms/Kiwi@195ea53 · GitHub	MISC	www.github.com	
huntr – Security Bounties for any GitHub repository	MISC	huntr.dev	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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