



CVE-2023-25156

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

Summary

CVE	CVE-2023-25156
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-15 15:15:00 UTC
Updated	2023-02-24 17:30:00 UTC
Description	Kiwi TCMS, an open source test management system, does not impose rate limits in versions prior to 12.0. This makes it e

Risk And Classification

Problem Types: CWE-307

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
No protection against brute-force attacks on login page · Advisory · kiwitcms/Kiwi · GitHub	MISC	github.com	
Rate limit everything under /accounts/ · kiwitcms/Kiwi@0ed213f · GitHub	MISC	github.com	
huntr: Page not found	MISC	huntr.dev	
Kiwi TCMS - Kiwi TCMS 12.0	MISC	kiwitcms.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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