



CVE-2023-33970

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-33970
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-05 20:15:00 UTC
Updated	2023-06-12 18:16:00 UTC
Description	Kanboard is open source project management software that focuses on the Kanban methodology. A vulnerability related to

Risk And Classification

Problem Types: CWE-862

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kanboard	Kanboard	All	All	All	All

References

Reference	Source	Link	T
Missing access control in internal task links feature · Advisory · kanboard/kanboard · GitHub	MISC	github.com	
Add missing permission check when creating/updating internal links · kanboard/kanboard@b501ef4 · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[691179](#) Free Berkeley Software Distribution (FreeBSD) Security Update for kanboard (bfca647c-0456-11ee-bafd-b42e991fc52e)

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