



CVE-2020-19825

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

Summary

CVE	CVE-2020-19825
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-15 22:15:00 UTC
Updated	2023-02-23 04:58:00 UTC
Description	Cross Site Scripting (XSS) vulnerability in kevinpapst kimai2 1.30.0 in /src/Twig/Runtime/MarkdownExtension.php, allows a

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kimai	Kimai	1.30.0	All	All	All

References

Reference

GitHub - kevinpapst/kimai2: Kimai v2 is a web-based multiuser time-tracking application. Free for everyone: freelancers, agencies, companies

fix possible xss in timesheet description by kevinpapst · Pull Request #962 · kimai/kimai · GitHub

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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