



CVE-2021-3983

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

Summary

CVE	CVE-2021-3983
State	PUBLIC
Assigner	security@huntr.dev
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-01 12:15:00 UTC
Updated	2021-12-02 20:17:00 UTC
Description	kimai2 is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kimai2 Project	Kimai2	All	All	All	All

References

Reference	Source	Link	Tags
Cross-site Scripting (XSS) - Stored vulnerability found in kimai2	CONFIRM	huntr.dev	
escape customer, project and activity name in javascript (#2959) · kevinpapst/kimai2@89bfa82 · GitHub	MISC	github.com	
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, 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