



CVE-2022-48110

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

Summary

CVE	CVE-2022-48110
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-13 20:15:00 UTC
Updated	2023-11-07 03:56:00 UTC
Description	** DISPUTED ** CKSource CKEditor 5 35.4.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the Fu

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ckeditor	Ckeditor	35.4.0	All	All	All

References

Reference	Source	Link	Tags
CKSource CKEditor5 35.4.0 Cross Site Scripting ≈ Packet Storm	MISC	packetstormsecurity.com	
HTML embed - CKEditor 5 Documentation	MISC	ckeditor.com	
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.

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