CVE-2023-38500

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2023-38500
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-07-25 21:15:00 UTC
Updated	2023-08-02 19:14:00 UTC
Description	TYPO3 HTML Sanitizer is an HTML sanitizer, written in PHP, aiming to provide cross-site-scripting-safe markup based on e

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Typo3	Html Sanitizer	All	All	All	All

References

Reference	Source	Link	Tags
Merge pull request from GHSA-59jf-3q9v-rh6g · TYPO3/html-sanitizer@e3026f5 · GitHub	MISC	github.com	
TYPO3-CORE-SA-2023-002: By-passing Cross-Site Scripting Protection in HTML Sanitizer	MISC	typo3.org	
By-passing Cross-Site Scripting Protection in HTML Sanitizer · Advisory · TYPO3/html-sanitizer · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

691230 Free Berkeley Software Distribution (FreeBSD) Security Update for typo3 (b1ac663f-3aa9-11ee-b887-b42e991fc52e)

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report