



CVE-2022-36020

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

Summary

CVE	CVE-2022-36020
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-13 17:15:00 UTC
Updated	2022-09-16 02:36:00 UTC
Description	The typo3/html-sanitizer package is an HTML sanitizer, written in PHP, aiming to provide XSS-safe markup based on explicit

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
typo3/html-sanitizer - Packagist	MISC	packagist.org	
[SECURITY] Correctly handle comment end bang state (#86) · TYPO3/html-sanitizer@60bfdc7 · GitHub	MISC	github.com	
masterminds/html5 - Packagist	MISC	packagist.org	
By-passing Cross-Site Scripting Protection in HTML Sanitizer · Advisory · TYPO3/html-sanitizer · GitHub	CONFIRM	github.com	
CVE Program record	CVE.ORG	www.cve.org	canor
NVD vulnerability detail	NVD	nvd.nist.gov	canor

No vendor comments have been submitted for this CVE.

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

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#)