



CVE-2022-31048

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

Summary

CVE	CVE-2022-31048
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-14 21:15:00 UTC
Updated	2022-06-23 13:16:00 UTC
Description	TYPO3 is an open source web content management system. Prior to versions 8.7.47 ELTS, 9.5.34 ELTS, 10.4.29, and 11.1.0 ELTS, there is a cross-site scripting (XSS) vulnerability in the form editor. This vulnerability allows an attacker to inject arbitrary HTML and JavaScript code into the form editor, which can be executed in the browser of the user viewing the form. This vulnerability affects all versions of TYPO3 from 8.7.47 ELTS to 11.1.0 ELTS.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
[SECURITY] Ensure text preview of multivalue items in form editor · TYPO3/typo3@6f2554d · GitHub	MISC	github.com	
TYPO3-CORE-SA-2022-003: Cross-Site Scripting in Form Framework	MISC	typo3.org	
Cross-Site Scripting in Form Framework · Advisory · TYPO3/typo3 · GitHub	CONFIRM	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.

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](#)