



CVE-2020-26216

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

Summary

CVE	CVE-2020-26216
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-17 21:15:00 UTC
Updated	2020-12-02 14:03:00 UTC
Description	TYPO3 Fluid before versions 2.0.8, 2.1.7, 2.2.4, 2.3.7, 2.4.4, 2.5.11 and 2.6.10 is vulnerable to Cross-Site Scripting. Three

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
[SECURITY] Introduce selective argument escaping · TYPO3/Fluid@f20db4e · GitHub	MISC	github.com	Patch, Third Party
TYPO3-CORE-SA-2020-009: Cross-Site Scripting through Fluid view helper arguments	MISC	typo3.org	Exploit, Vendor Ad
Cross-Site Scripting through Fluid view helper arguments · Advisory · TYPO3/Fluid · GitHub	CONFIRM	github.com	Exploit, Third Party
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.

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)