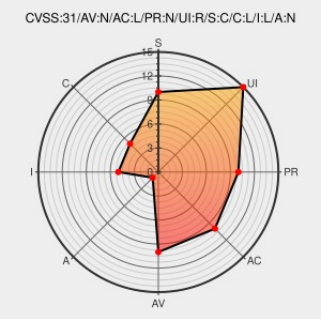
# CVE-2020-26227

Published on: 11/23/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:56 PM UTC

## **CVE-2020-26227** - advisory for GHSA-vqqx-jw6p-q3rf

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Typo3 from Typo3 contain the following vulnerability:

TYPO3 is an open source PHP based web content management system. In TYPO3 before versions 9.5.23 and 10.4.10 the system extension Fluid (typo3/cms-fluid) of the TYPO3 core is vulnerable to cross-site scripting passing user-controlled data as argument to Fluid view helpers. Update to TYPO3 versions 9.5.23 or 10.4.10 that fix the problem described.

CVE-2020-26227 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **TYPO3** - **TYPO3.CMS** version **>= 9.0.0, < 9.5.23**

Affected Vendor/Software: **TYPO3** - **TYPO3.CMS** version **>= 10.0.0, < 10.4.10**

### CVSS3 Score: 6.1 - MEDIUM

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| NETWORK | LOW | NONE | REQUIRED |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| CHANGED | LOW | LOW | NONE |

### CVSS2 Score: 4.3 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | MEDIUM | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| NONE | PARTIAL | NONE |

## CVE References

| Description | Tags | Link |
|---|---|---|
| Cross-Site Scripting in Fluid view helpers · Advisory · TYPO3/TYPO3.CMS · GitHub | Exploit<br>Third Party Advisory<br>github.com<br>text/html | CONFIRM github.com/TYPO3/TYPO3.CMS/security/advisories/GHSA-vqqx-jw6p-q3rf |
| TYPO3-CORE-SA-2020-010: Cross-Site Scripting in Fluid view helpers | Exploit<br>Vendor Advisory<br>typo3.org<br>text/html | MISC typo3.org/security/advisory/typo3-core-sa-2020-010 |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:typo3:typo3:*:*:*:*:*:*:*:*:

cpe:2.3:a:typo3:typo3:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→