Cross-Site Scripting in Fluid view helpers

Moderate **ohader** published **GHSA-vqqx-jw6p-q3rf** on Nov 17, 2020

Package

php **typo3/cms-core** (Composer)

Affected versions	Patched versions
9.0.0-9.5.22, 10.0.0-10.4.9	9.5.23, 10.4.10

Description

Meta

- CVSS: `CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:F/RL:O/RC:C` (5.7)
- CWE-79

Problem

It has been discovered that 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.

```
<f:form ... fieldNamePrefix="{payload}" />
<f:be.labels.csh ... label="{payload}" />
<f:be.menus.actionMenu ... label="{payload}" />
```

Solution

Update to TYPO3 versions 9.5.23 or 10.4.10 that fix the problem described.

Credits

Thanks to TYPO3 security team member Oliver Hader who reported this issue and to TYPO3 security team members Helmut Hummel & Oliver Hader who fixed the issue.

References

- TYPO3-CORE-SA-2020-010

Severity

Moderate

CVE ID

CVE-2020-26227

Weaknesses

No CWEs

Credits

ohader