Cross-Site Scripting in ternary conditional operator

Moderate **ohader** published **GHSA-7733-hjv6-4h47** on Oct 7, 2020

Package

php **typo3fluid/fluid** (Composer)

Affected versions

2.0.0-2.0.4, 2.1.0-2.1.3, 2.2.0, 2.3.0-2.3.4, 2.4.0, 2.5.0-2.5.4, 2.6.0

Patched versions

2.0.5, 2.1.4, 2.2.1, 2.3.5, 2.4.1, 2.5.5, 2.6.1

Description

Meta

- CVSS: `CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:N/E:F/RL:O/RC:C` (5.0)
- CWE-79

This vulnerability has been fixed in May 2019 already, CVE and GHSA were assigned later in October 2020

Problem

It has been discovered that the Fluid Engine (package `typo3fluid/fluid`) is vulnerable to cross-site scripting when making use of the ternary conditional operator in templates like the following.

```
{showFullName ? fullName : defaultValue}
```

Solution

Update to versions 2.0.5, 2.1.4, 2.2.1, 2.3.5, 2.4.1, 2.5.5 or 2.6.1 of this `typo3fluid/fluid` package that fix the problem described.

Updated versions of this package are bundled in following TYPO3 (`typo3/cms-core`) releases:

- TYPO3 v8.7.25 (using `typo3fluid/fluid` v2.5.5)
- TYPO3 v9.5.6 (using `typo3fluid/fluid` v2.6.1)

Credits

Thanks to Bill Dagou who reported this issue and to TYPO3 core merger Claus Due who fixed the issue.

References

- TYPO3-CORE-SA-2019-013

Severity

Moderate

CVE ID

CVE-2020-15241

Weaknesses

No CWEs

Credits

billdagou

NamelessCoder