Tue. 17th November, 2020

TYPO3-CORE-SA-2020-010: Cross-Site Scripting in Fluid view helpers

Categories: Development (/help/security-advisories/development), TYPO3 CMS (/help/security-advisories/typo3-cms)
Created by Oliver Hader

It has been discovered that TYPO3 CMS is vulnerable to cross-site scripting..

- **Component Type:** TYPO3 CMS
- **Subcomponent:** Fluid (ext:fluid)
- **Release Date:** November 17, 2020
- **Vulnerability Type:** Cross-Site Scripting
- **Affected Versions:** 10.0.0-10.4.9, 9.0.0-9.5.22, 8.7.0-8.7.37 ELTS, 7.6.0-7.6.47 ELTS, 6.2.0-6.2.53 ELTS
- **Severity:** Medium
- **Suggested 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 (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:F/RL:O/RC:C&version=3.1)
- **References:** CVE-2020-26227 (https://nvd.nist.gov/vuln/detail/CVE-2020-26227), CWE-79 (https://cwe.mitre.org/data/definitions/79.html)

Problem Description

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 10.4.10, 9.5.23, 8.7.38 ELTS, 7.6.48 ELTS or 6.2.54 ELTS ELTS 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.

General Advice

Follow the recommendations that are given in the TYPO3 Security Guide (https://docs.typo3.org/typo3cms/CoreApiReference/Security/Index.html#security). Please subscribe to the typo3-announce (http://lists.typo3.org/cgi-bin/mailman/listinfo/typo3-announce) mailing list.

General Note

All security related code changes are tagged so that you can easily look them up in our review system (https://review.typo3.org/#/q/status:merged+project:Packages/TYPO3.CMS+topic:security,n,z).