Cross-Site Scripting in Content Rendering

Moderate **benjaminkott** published **GHSA-p48w-vf3c-rqjx** on Apr 27, 2021

Package

php **bk2k/bootstrap-package** (Composer)

Affected versions	Patched versions
7.1.0-7.1.1, 8.0.0-8.0.7, 9.0.0-9.0.3, 9.1.0-9.1.2, 10.0.0-10.0.9, 11.0.0-11.0.2	7.1.2, 8.0.8, 9.0.4, 9.1.3, 10.0.10, 11.0.3

Description

Meta

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

Problem

It has been discovered that rendering content in the website frontend is vulnerable to cross-site scripting. A valid backend user account is needed to exploit this vulnerability.

The following templates are affected by the vulnerability:

- `Resources/Private/Partials/ContentElements/Carousel/Item/CallToAction.html`
- `Resources/Private/Partials/ContentElements/Carousel/Item/Header.html`
- `Resources/Private/Partials/ContentElements/Carousel/Item/Text.html`
- `Resources/Private/Partials/ContentElements/Carousel/Item/TextAndImage.html`
- `Resources/Private/Partials/ContentElements/Header/SubHeader.html`

Users of the extension, who have overwritten the affected templates with custom code must manually apply the security fix as shown in this Git commit.

Solution

Update to version 7.1.2, 8.0.8, 9.0.4, 9.1.3, 10.0.10 or 11.0.3 of the Bootstrap Package that fix the problem described.

Updated version are available from the TYPO3 extension manager, Packagist and at https://extensions.typo3.org/extension/download/bootstrap_package/.

Credits

Thanks to TYPO3 security team member Oliver Hader who reported and fixed the issue.

References

- TYPO3-EXT-SA-2021-007

Severity

Moderate

CVE ID

CVE-2021-21365

Weaknesses

CWE-79

Credits

ohader