Tue. 27th April, 2021

TYPO3-EXT-SA-2021-007: Cross-Site Scripting in extension "Bootstrap Package" (bootstrap_package)

Categories: Development (/help/security-advisories/development), Security (/help/security-advisories/security)
Created by Torben Hansen

It has been discovered that the extension "Bootstrap Package" (bootstrap_package) is susceptible to Cross-Site Scripting.

- Release Date: April 27, 2021
- Component Type: Third party extension. This extension is not a part of the TYPO3 default installation.
- Component: "Bootstrap Package" (bootstrap_package)
- Vulnerability Type: Cross-Site Scripting
- Affected Versions: 11.0.0 - 11.0.2, 10.0.0 - 10.0.9, 9.0.0-9.0.3, 9.1.0-9.1.2, 8.0.0 - 8.0.7, 7.1.1 and below
- Severity: Medium
- Suggested 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 (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N/E:F/RL:O/RC:C&version=3.1)
- References: CVE-2021-21365 (https://nvd.nist.gov/vuln/detail/CVE-2021-21365)

Problem Description

The extension fails to properly encode user input for output in HTML context. 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 must manually apply required changes as shown below:

Vulnerable:
<f:format.htmlentitiesDecode>{userInput}</f:format.htmlentitiesDecode>

Not vulnerable:
<f:format.htmlspecialchars doubleEncode="false">{userInput}</f:format.htmlspecialchars>

Solution

Updated versions 7.1.2, 8.0.8, 9.0.4, 9.1.3, 10.0.10, 11.0.3 are available from the TYPO3 extension manager, Packagist and at
https://extensions.typo3.org/extension/download/bootstrap_package/7.1.2/zip (https://extensions.typo3.org/extension/download/bootstrap_package/7.1.2/zip)
https://extensions.typo3.org/extension/download/bootstrap_package/8.0.8/zip (https://extensions.typo3.org/extension/download/bootstrap_package/8.0.8/zip)
https://extensions.typo3.org/extension/download/bootstrap_package/9.0.4/zip (https://extensions.typo3.org/extension/download/bootstrap_package/9.0.4/zip)
https://extensions.typo3.org/extension/download/bootstrap_package/9.1.3/zip (https://extensions.typo3.org/extension/download/bootstrap_package/9.1.3/zip)
https://extensions.typo3.org/extension/download/bootstrap_package/10.0.10/zip (https://extensions.typo3.org/extension/download/bootstrap_package/10.0.10/zip)
https://extensions.typo3.org/extension/download/bootstrap_package/11.0.3/zip (https://extensions.typo3.org/extension/download/bootstrap_package/11.0.3/zip)
Users of the extension are advised to update the extension as soon as possible.

Credits

Thanks to TYPO3 Security Team Member Oliver Hader who reported and 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-guidelines). Please subscribe to the typo3-announce (http://lists.typo3.org/cgi-bin/mailman/listinfo/typo3-announce) mailing list.