[CVE-2022-27777] Possible XSS Vulnerability in Action View tag helpers

Aaron Patterson tenderlove core team Apr 26

There is a possible XSS vulnerability in Action View tag helpers. Passing untrusted input as hash keys can lead to a possible XSS vulnerability. This vulnerability has been assigned the CVE identifier CVE-2022-27777.

- Versions Affected: ALL
- Not affected: NONE
- Fixed Versions: 7.0.2.4, 6.1.5.1, 6.0.4.8, 5.2.7.1

Impact

If untrusted data is passed as the hash key for tag attributes, there is a possibility that the untrusted data may not be properly escaped which can lead to an XSS vulnerability.

Impacted code will look something like this:

```
check_box_tag('thename', 'thevalue', false, aria: { malicious_input => 'theval
```

Where the “malicious_input” variable contains untrusted data.

All users running an affected release should either upgrade or use one of the workarounds immediately.

Releases

The FIXED releases are available at the normal locations.

Workarounds

Escape the untrusted data before using it as a key for tag helper methods.

Patches

To aid users who aren’t able to upgrade immediately we have provided patches for the two supported release series. They are in git-am format and consist of a single changeset.

Skip to main content

- 5-2-tag-helper-xss.patch - Patch for 5.2 series

- 6-0-tag-helper-xss.patch - Patch for 6.0 series
- 6-1-tag-helper-xss.patch - Patch for 6.1 series
- 7-0-tag-helper-xss.patch - Patch for 7.0 series

Credits

Thank you to **Álvaro Martín Fraguas** for reporting the issue and providing patches!

5-2-tag-helper-xss.patch (16.2 KB) **6-0-tag-helper-xss.patch** (15.7 KB) **6-1-tag-helper-xss.patch** (19.8 KB) **7-0-tag-helper-xss.patch** (19.9 KB)

More Resources

Keep up to date with **Rails on Twitter** and **This Week in Rails**

Policies: **Conduct**, **License**, **Maintenance**, **Security**, **Trademarks**