Stored XSS via Notification Body with Zero-Click Execution on Login

Moderate **dasgarner** published **GHSA-85w9-c833-q4w2** 12 hours ago

Package

xibo-cms

Affected versions

<= 4.4.0

Patched versions

4.4.1

Description

Impact

A stored Cross-Site Scripting (XSS) vulnerability in Xibo CMS allows an authenticated user with notification creation permissions to inject arbitrary JavaScript into the notification body. When the notification is set as an "interrupt," the payload executes automatically in the browser of any targeted user upon login, requiring zero user interaction.

Exploitation of the vulnerability is possible on behalf of an authorized user who has both of the following privileges, which are not granted to non-admins as standard:
- Access to the Notification Centre to view past notifications
- Include "Add Notification" button to allow for the creation of new notifications

Patches

Users should upgrade to version 4.4.1 which fixes this issue.

Workarounds

Upgrading to a fixed version is necessary to remediate. Users unable to upgrade should revoke such privileges from users they do not trust.

Disclosure timeline (UTC)

- 3rd March 2026: Responsible disclosure

- 5th March 2026: Acknowledgement and provision of a patch
- 24th March 2026: Available in a release
- 23rd April 2026: Public disclosure

Acknowledgements

The vulnerability was discovered by Swarnim Bandekar
https://github.com/swarnimbandekar

Severity

Moderate 6.4 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Changed
Confidentiality	Low
Integrity	Low
Availability	None

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N

CVE ID

CVE-2026-31953

Weaknesses

▶ CWE-79

Credits

swarnimbandekar Reporter