SQL Injection via DataSet Filter Parameter in Xibo CMS API

High **dasgarner** published **GHSA-rq92-f6fv-3629** 12 hours ago

Package

xibosignage/xibo-cms

Affected versions

>1.7 <=4.4.0

Patched versions

4.4.1

Description

Impact

An SQL injection vulnerability was discovered in the API routes inside the CMS responsible for Filtering DataSets. This allows an authenticated user to to obtain and modify arbitrary data from the Xibo database by injecting specially crafted values in to the API filter parameter.

Exploitation of the vulnerability is possible on behalf of an authorized user who has either of the following privileges:
- Access to DataSet Feature
- Access to the Layout Feature

Patches

Users should upgrade to version 4.3.1 which fixes this issue. Customers who host their CMS with Xibo Signage have been patched if they are using 4.4, 4.3, 3.3, 2.3 or 1.8.

Workarounds

Upgrading to a fixed version is necessary to remediate.

Patches are available for earlier versions of Xibo CMS that are out of support:

- 3.3 patch
- 2.3 patch

- 1.8 patch

Disclosure timeline (UTC)

- 3rd March 2026: Responsible disclosure
- 4th 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

High 7.6 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-31952

Weaknesses

- CWE-89
- CWE-184

Credits

swarnimbandekar Reporter