# Authenticated Server-Side Request Forgery (SSRF) in Remote DataSet Functionality

Moderate **dasgarner** published **GHSA-5q58-9vhx-xg2p** 12 hours ago

**Package**

**xibosignage/xibo-cms**

| Affected versions | Patched versions |
| --- | --- |
| <=4.4.0 | 4.4.1 |

## Description

### Impact

An authenticated Server-Side Request Forgery (SSRF) vulnerability in the Xibo CMS allows users with DataSet permissions to make arbitrary HTTP requests from the CMS server to internal or external network resources. This can be exploited to scan internal infrastructure, access local cloud metadata endpoints (e.g., AWS IMDS), interact with internal services that lack authentication, or exfiltrate data.

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:
- Include "Add DataSet" button to allow for additional DataSets to be created independently to Layouts

### 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
- 9th 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 4.9 / 10

**CVSS v3 base metrics**

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

Learn more about base metrics

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

**CVE ID**

CVE-2026-31955

**Weaknesses**

▶ CWE-918

**Credits**

swarnimbandekar Reporter