



# ChurchCRM has Stored XSS in Group Name

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2026-35575
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-07 18:16:42 UTC
<b>Updated</b>	2026-04-09 18:47:25 UTC
<b>Description</b>	ChurchCRM is an open-source church management system. Prior to 6.5.3, a Stored Cross-Site Scripting (Stored XSS) vuln

## Risk And Classification

**Primary CVSS:** v3.1 8 HIGH from security-advisories@github.com

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

**EPSS:** 0.000380000 probability, percentile 0.113770000 (date 2026-04-09)

**Problem Types:** CWE-79 | CWE-1004 | CWE-79 CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | CWE-1004 CWE-1004: Sensitive Cookie Without 'HttpOnly' Flag

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Unchanged

Confidentiality

High

High

Integrity

High

Availability

High

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Churchcrm	Churchcrm	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	ChurchCRM	CRM	affected < 6.5.3	Not specified

### References

Reference	Source	Link	Tags
github.com/ChurchCRM/CRM/security/advisories/GHSA-gc8q-2gw7-qj7w	security-advisories@github.com	github.com	Third Party Adv
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)