ChurchCRM has Stored XSS in Group Name

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

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

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

ntegrity

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, analy

No vendor comments have been submitted for this CVE.

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