



# ChurchCRM has a Stored XSS in Person Profile - Add a Note

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#) 

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2026-35574  |
| <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 17:16:32 UTC   |
| <b>Updated</b>         | 2026-04-07 18:16:41 UTC   |
| <b>Description</b>     | ChurchCRM is an open-source church management system. Prior to 6.5.3, a stored Cross-Site Scripting (XSS) vulnerability |

## Risk And Classification

**Primary CVSS:** v3.1 7.3 HIGH from security-advisories@github.com

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

**Problem Types:** CWE-79 | CWE-79 CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

| Version | Source                         | Type      | Score | Severity | Vector                                       |
|---------|--------------------------------|-----------|-------|----------|--|
| 3.1     | security-advisories@github.com | Secondary | 7.3   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N |
| 3.1     | CNA                            | DECLARED  | 7.3   | HIGH     | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N |

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Privileges Required

**Low**

User Interaction

**Required**

Scope

**Unchanged**

Confidentiality

**High**

Integrity

High

Availability

None

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

### 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-cx82-8xrh-7f5c | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | <a href="#">github.com</a>   |         |
| CVE Program record   | CVE.ORG                              | <a href="#">www.cve.org</a>  | canonic |
| NVD vulnerability detail   | NVD                                  | <a href="#">nvd.nist.gov</a> | canonic |

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](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)