ChurchCRM has a Path traversal leads to RCE

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

Summary

CVE	CVE-2026-35573
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-07 18:16:41 UTC
Updated	2026-04-10 20:59:20 UTC
Description	ChurchCRM is an open-source church management system. Prior to 6.5.3, a path traversal vulnerability in ChurchCRM's ba

Risk And Classification

Primary CVSS: v3.1 9.1 CRITICAL from security-advisories@github.com

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

EPSS: 0.002580000 probability, percentile 0.491530000 (date 2026-04-12)

Problem Types: CWE-22 | CWE-434 | CWE-22 CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | CWE-434 CWE-434: Unrestricted Upload of File with Dangerous Type

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	DECLARED	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Changed

Confidentiality

High

High

ntegrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/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-r6cr-mvr9-f6wx	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com	Exploit,
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

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