ChurchCRM: Authenticated Remote Code Execution via Unrestricted PHP File Write in Database Restore Function

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

Summary

CVE	CVE-2026-40484
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-18 00:16:39 UTC
Updated	2026-04-18 00:16:39 UTC
Description	ChurchCRM is an open-source church management system. In versions prior to 7.2.0, the database backup restore functio

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

Problem Types: CWE-269 | CWE-434 | CWE-552 | CWE-269 CWE-269: Improper Privilege Management | CWE-434 CWE-434: Unrestricted Upload of File with Dangerous Type | CWE-552 CWE-552: Files or Directories Accessible to External Parties

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

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	ChurchCRM	CRM	affected < 7.2.0	Not specified

References

Reference	Source	Link	Ta
github.com/ChurchCRM/CRM/security/advisories/GHSA-2932-77f9-62fx	security-advisories@github.com	github.com	
github.com/ChurchCRM/CRM/pull/8610	security-advisories@github.com	github.com	
github.com/ChurchCRM/CRM/commit/68be1d12bc4cc1429575ae797ef05efe47030d39	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

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