Authenticated SQL Injection in `/api/families/byCheckNumber/{scanString}`

High **DawoudIO** published **GHSA-hc37-vx3w-34fg** last week

Package

php **ChurchCRM/CRM** (Composer)

Affected versions

<= 7.1.2

Patched versions

7.2.0

Description

Overview

SQL injection in `FinancialService::getMemberByScanString()` via unsanitized `$routeAndAccount` concatenated into raw SQL.

Fix

✅ Patched in 7.2.0 — PR #8607 (merged as `214694eb83`)

Replaced raw SQL with `FamilyQuery::findOneByScanCheck()` Propel ORM method.

Severity

High

CVE ID

CVE-2026-40482

Weaknesses

No CWEs

Credits

HuajiHD Reporter