

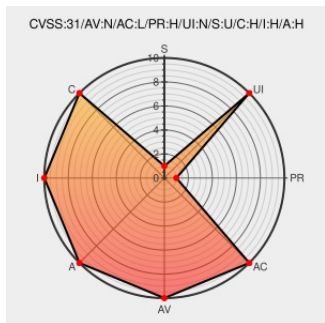


CVE-2022-31325

Published on: Not Yet Published

Last Modified on: 11/29/2022 04:40:00 PM UTC

CVE-2022-31325

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Churchcrm](#) from [Churchcrm](#) contain the following vulnerability:

There is a SQL Injection vulnerability in ChurchCRM 4.4.5 via the 'PersonID' field in /churchcrm/WhyCameEditor.php.

CVE-2022-31325 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.2 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
ChurchCRM 4.4.5 SQL Injection ~ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/167483/ChurchCRM-4.4.5-SQL-Injection.html
SQL Injection vulnerability in ChurchCRM 4.4.5 via	github.com	MISC

/churchcrm/WhyCameEditor.php · Issue #6005 · ChurchCRM/CRM · GitHub	text/html	github.com/ChurchCRM/CRM/issues/6005
CVE-mitre/2022/CVE-2022-31325 at main · nu11secur1ty/CVE-mitre · GitHub	github.com text/html	MISC github.com/nu11secur1ty/CVE-mitre/tree/main/2022/CVE-2022-31325
nu11secur1ty	www.nu11secur1ty.com text/html Inactive Link Not Archived	MISC www.nu11secur1ty.com/2022/06/cve-2022-31325.htm

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

There is a SQL Injection vulnerability in ChurchCRM 4.4.5 via the 'PersonID' field in /churchcrm/WhyCameEditor.php. C...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Churchcrm	Churchcrm	4.4.5	All	All	All
cpe:2.3:a:churchcrm:churchcrm:4.4.5:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-31325 : There is a SQL Injection vulnerability in ChurchCRM 4.4.5 via the 'PersonID' field in /churchcrm/W... twitter.com/i/web/status/1...	2022-06-08 16:08:13
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-31325 There is a SQL Injection vulnerability in ChurchCRM 4.4.5 via the... twitter.com/i/web/status/1...	2022-06-08 18:56:01
@LinInfoSec	Php - CVE-2022-31325: github.com/ChurchCRM/CRM/...	2022-06-08 20:02:49
@phpadvisories	CVE-2022-31325 ChurchCRM 4.4.5 WhyCameEditor.php PersonID SQL Injection (ID 6005) zpr.io/nhiE7DvTWuDu #phpsec	2022-06-09 09:16:47
/r/netcve	CVE-2022-31325	2022-06-08 17:38:22

[← Previous ID](#)

[Next ID →](#)

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](#).

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