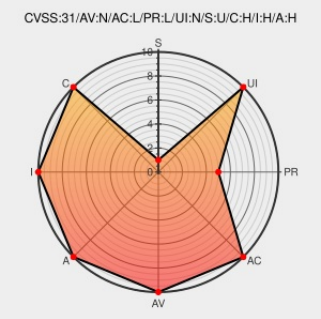
CVE-2021-43258

Published on: Not Yet Published

Last Modified on: 11/30/2022 03:52:00 PM UTC

CVE-2021-43258

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Churchinfo from Churchdb contain the following vulnerability:

CartView.php in ChurchInfo 1.3.0 allows attackers to achieve remote code execution through insecure uploads. This requires authenticated access tot he ChurchInfo application. Once authenticated, a user can add names to their cart, and compose an email. Uploading an attachment for the email stores the attachment on the site in the /tmp_attach/ folder where it can be accessed with a GET request. There are no limitations on files that can be attached, allowing for malicious PHP code to be uploaded and interpreted by the server.

CVE-2021-43258 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVE References

Description	Tags	Link
ChurchInfo open source church database created with PHP & MySQL! - ChurchInfo open source church database created with PHP & MySQL!	www.churchdb.org text/html	MISC www.churchdb.org/
Adding exploit for ChurchInfo 1.2.13-1.3.0 RCE (CVE-2021-43258) by m4lwhere · Pull Request #17257 · rapid7/metasploit-framework · GitHub	github.com text/html	MISC github.com/rapid7/metasploit-framework/pull/17257
ChurchInfo - Browse Files at SourceForge.net	sourceforge.net text/html	MISC sourceforge.net/projects/churchinfo/files/

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

ChurchInfo 1.2.13-1.3.0 Remote Code Execution Exploit

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Churchdb	Churchinfo	All	All	All	All

cpe:2.3:a:churchdb:churchinfo:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-43258 : CartView.php in ChurchInfo 1.3.0 allows attackers to achieve remote code execution through insecur… twitter.com/i/web/status/1…	2022-11-23 19:06:23
@JohnJasonFallow	New vulnerability on the NVD: CVE-2021-43258 ift.tt/g3u6PV2	2022-11-23 21:16:27
/r/netcve	CVE-2021-43258	2022-11-23 19:38:16

← Previous ID

Next ID→