



# CVE-2021-43258

Published on: Not Yet Published

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

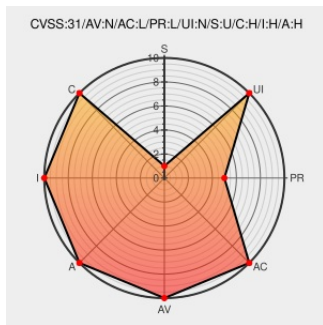
## CVE-2021-43258

[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 to the 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 [M](#) [cve@mitre.org](mailto: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
<b>NETWORK</b>	<b>LOW</b>	<b>LOW</b>	<b>NONE</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>UNCHANGED</b>	<b>HIGH</b>	<b>HIGH</b>	<b>HIGH</b>

## CVE References

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

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

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](mailto: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	<a href="#">Churchdb</a>	<a href="#">Churchinfo</a>	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 insecure... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2022-11-23 19:06:23
 @JohnJasonFallow	New vulnerability on the NVD: CVE-2021-43258 <a href="https://ift.tt/g3u6PV2">ift.tt/g3u6PV2</a>	2022-11-23 21:16:27
 /r/netcve	<a href="#">CVE-2021-43258</a>	2022-11-23 19:38:16

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)