



CVE-2022-4252

Published on: Not Yet Published

Last Modified on: 12/02/2022 06:41:00 PM UTC

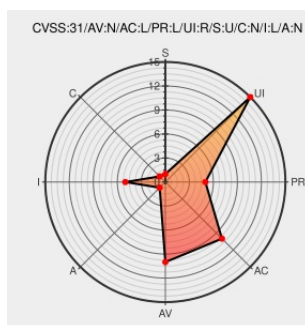
CVE-2022-4252

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Canteen Management System](#) from [Canteen Management System Project](#) contain the following vulnerability:

A vulnerability was found in SourceCodester Canteen Management System. It has been classified as problematic. This affects the function builtin_echo of the file categories.php. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-214629 was assigned to this vulnerability.

CVE-2022-4252 has been assigned by cna@vuldb.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **SourceCodester - Canteen Management System** version **n/a**

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVE References

Description	Tags	Link
CVE-2022-4252 SourceCodester Canteen Management System categories.php builtin_echo cross site scripting	vuldb.com text/html Inactive Link Not Archived	MISC vuldb.com/?id.214629
SourceCodester Canteen Management System categories.php builtin_echo cross site scripting_@sec的博客-CSDN博客	blog.csdn.net text/html	MISC blog.csdn.net/weixin_43864034/article/details/128127288

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Canteen Management System Project	Canteen Management System	-	All	All	All
cpe:2.3:a:canteen_management_system_project:canteen_management_system:-:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-4252 : A vulnerability was found in SourceCodester Canteen Management System. It has been classified as pr... twitter.com/i/web/status/1...	2022-12-01 08:09:55
 @threatmeter	CVE-2022-4252 SourceCodester Canteen Management System categories.php builtin_echo cross site scripting A vulnera... twitter.com/i/web/status/1...	2022-12-01 08:50:37
 @ColorTokensInc	Emerging Vulnerability Found CVE-2022-4252 - A vulnerability was found in SourceCodester Canteen Management System.... twitter.com/i/web/status/1...	2022-12-01 08:50:44
 /r/netcve	CVE-2022-4252	2022-12-01 09:38:51

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#)