

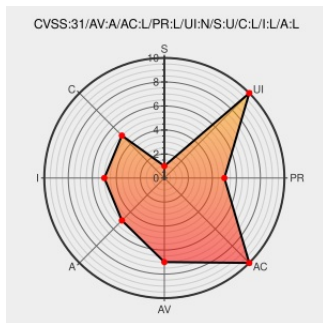


CVE-2022-2708

Published on: Not Yet Published

Last Modified on: 08/12/2022 04:04:00 PM UTC

CVE-2022-2708

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

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

A vulnerability, which was classified as critical, was found in SourceCodester Gym Management System. This affects an unknown part of the file login.php. The manipulation of the argument user_login with the input 123@xx.com' OR (SELECT 9084 FROM(SELECT COUNT(*),CONCAT(0x7178767871,(SELECT

(ELT(9084=9084,1))),0x71767a6271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- dPvW leads to sql injection. Access to the local network is required for this attack. The exploit has been disclosed to the public and may be used. The identifier VDB-205833 was assigned to this vulnerability.

CVE-2022-2708 has been assigned by [cna@vuldb.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [SourceCodester](#) - [Gym Management System](#) version n/a

CVSS3 Score: **9.8 - CRITICAL**

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

CVE References

Description	Tags	Link
CVE-2022-2708 SourceCodester Gym Management System login.php sql injection	vuldb.com text/html	MISC vuldb.com/?id.205833

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 our linked reports to [cna@vuldb.com](#).

CVE.report 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	Gym Management System Project	Gym Management System	-	All	All	All
cpe:2.3:a:gym_management_system_project:gym_management_system:-:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @phpadvisories	CVE-2022-2708 SourceCodester Gym Management System login.php user_login sql injection zpr.io/JHjEs6DGHjDK #phpsec	2022-08-08 07:20:43
 @CVEreport	CVE-2022-2708 : A vulnerability, which was classified as critical, was found in SourceCodester Gym Management System... twitter.com/i/web/status/1...	2022-08-08 12:58:22
 @LinInfoSec	Php - CVE-2022-2708: vuldb.com/?id.205833	2022-08-08 15:01:16
 @threatmeter	CVE-2022-2708 A vulnerability, which was classified as critical, was found in SourceCodester Gym Management System.... twitter.com/i/web/status/1...	2022-08-09 07:09:41
 /r/netcve	CVE-2022-2708	2022-08-08 14:38:40

[← 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](#)