

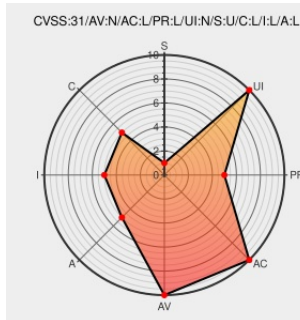


CVE-2022-2489

Published on: Not Yet Published

Last Modified on: 07/26/2022 10:20:00 PM UTC

CVE-2022-2489

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

Certain versions of [Simple E-learning System](#) from [Simple E-learning System Project](#) contain the following vulnerability:

A vulnerability was found in SourceCodester Simple E-Learning System 1.0. It has been rated as critical. This issue affects some unknown processing of the file classRoom.php. The manipulation of the argument classCode with the input `1'|(SELECT 0x6770715a WHERE 8795=8795 AND (SELECT 8342 FROM(SELECT`

`COUNT(*),CONCAT(0x7171786b71,(SELECT (ELT(8342=8342,1))),0x717a7a7671,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)|'` leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.

CVE-2022-2489 has been assigned by [cna@vuldb.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [SourceCodester](#) - **Simple E-Learning System** version 1.0

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
CVE-2022-2489 SourceCodester Simple E-Learning System classRoom.php sql injection	vuldb.com text/html	MISC vuldb.com/?id.204551
CVEproject/Simple-E-Learning-System.md at main · xiahao90/CVEproject · GitHub	github.com text/html	MISC github.com/xiahao90/CVEproject/blob/main/xiahao.webray.com.cn/Simple-E-Learning-System.md

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	Simple E-learning System Project	Simple E-learning System	1.0	All	All	All
cpe:2.3:a:simple_e-learning_system_project:simple_e-learning_system:1.0:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-2489 : A vulnerability was found in SourceCodester Simple E-Learning System 1.0. It has been rated as crit... twitter.com/i/web/status/1...	2022-07-20 11:43:53
 @LinInfoSec	Php - CVE-2022-2489: github.com/xiahao90/CVEpr...	2022-07-20 16:00:08
 @threatmeter	CVE-2022-2489 A vulnerability was found in SourceCodester Simple E-Learning System 1.0. It has been rated as critic... twitter.com/i/web/status/1...	2022-07-21 07:09:38
 /r/netcve	CVE-2022-2489	2022-07-20 12:38:26

[← 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](#)