



CVE-2020-14972

Published on: 06/22/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:00 PM UTC

CVE-2020-14972

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



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

Multiple SQL injection vulnerabilities in Sourcecodester Pisay Online E-Learning System 1.0 allow remote unauthenticated attackers to bypass authentication and achieve Remote Code Execution (RCE) via the user_email, user_pass, and id parameters on the admin login-portal and the edit-lessons webpages.

CVE-2020-14972 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

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

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Free Source Code Projects and Tutorials - sourcecodester.com	Vendor Advisory www.sourcecodester.com text/html	MISC www.sourcecodester.com

Pisay Online E-Learning System 1.0 - Remote Code Execution - PHP webapps Exploit

Exploit

Third Party Advisory

VDB Entry

www.exploit-db.com

Proof of Concept

text/html

MISC www.exploit-db.com/exploits/48439

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	Pisay Online E-learning System Project	Pisay Online E-learning System	1.0	All	All	All
Application	Pisay Online E-learning System Project	Pisay Online E-learning System	1.0	All	All	All

cpe:2.3:a:pisay_online_e-learning_system_project:pisay_online_e-learning_system:1.0:*:*:*:*:*:

cpe:2.3:a:pisay_online_e-learning_system_project:pisay_online_e-learning_system:1.0:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← 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](#)