



VDB-354250 · CVE-2026-5182 · GCVE-100-354250

SOURCECODESTER TEACHER RECORD SYSTEM 1.0 PARAMETER SEARCHTEACHER SQL INJECTION

CVSS Meta Temp Score ?

6.6

Current Exploit Price (≈) ?

\$0-\$5k

CTI Interest Score ?

1.71

Summary

A vulnerability categorized as **critical** has been discovered in **SourceCodester Teacher Record System 1.0**. The affected element is an unknown function of the file *Teacher Record System* of the component *Parameter Handler*. Executing a manipulation of the argument *searchteacher* can lead to sql injection. This vulnerability is registered as **CVE-2026-5182**. It is possible to launch the attack remotely. Furthermore, an exploit is available.

Details

A vulnerability classified as critical was found in **SourceCodester Teacher Record System 1.0**. This vulnerability affects an unknown functionality of the file *Teacher Record System* of the component *Parameter Handler*. The manipulation of the argument *searchteacher* with an unknown input leads to a sql injection vulnerability. The CWE definition for the vulnerability is **CWE-89**. The product constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component. As an impact it is known to affect confidentiality, integrity, and availability.

The advisory is available at github.com. This vulnerability was named **CVE-2026-5182**. The exploitation appears to be easy. The attack can be initiated remotely. No form of authentication is required for a successful exploitation. Technical details and also a public exploit are known. This vulnerability is assigned to **T1505** by the MITRE ATT&CK project.

It is possible to download the exploit at github.com. It is declared as proof-of-concept.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

Similar entries are available at [VDB-354203](https://vuldb.com/vuln/354203), [VDB-354206](https://vuldb.com/vuln/354206), [VDB-354207](https://vuldb.com/vuln/354207) and [VDB-354208](https://vuldb.com/vuln/354208).

Product

Vendor

- [SourceCodester](#)

Name

- [Teacher Record System](#)

Version

- [1.0](#)

License

- [free](#)

Website

- Vendor: <https://www.sourcecodester.com/>

CPE 2.3

- 

CPE 2.2

- 

CVSSv4

VulDB Vector: 

VulDB Reliability: 

CVSSv3

VulDB Meta Base Score: 7.3

VulDB Meta Temp Score: 6.6

VulDB Base Score: 7.3

VulDB Temp Score: 6.6

VulDB Vector: 

VulDB Reliability: 

CVSSv2



VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Sql injection
CWE: [CWE-89](#) / [CWE-74](#) / [CWE-707](#)
CAPEC: 🔒
ATT&CK: 🔒

Physical: No
Local: No
Remote: Yes

Availability: 🔒
Access: Public
Status: Proof-of-Concept
Download: 🔒
Price Prediction: 🔍
Current Price Estimation: 🔒



Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: no mitigation known

Status: 🔍

0-Day Time: 🗝️

Timeline

03/30/2026		Advisory disclosed
03/30/2026	+0 days	VulDB entry created
03/30/2026	+0 days	VulDB entry last update

Sources

Vendor: sourcecodester.com

Advisory: github.com

Status: Not defined

CVE: [CVE-2026-5182](#) (🗝️)

GCVE (CVE): [GCVE-0-2026-5182](#)

GCVE (VulDB): [GCVE-100-354250](#)

scip Labs: <https://www.scip.ch/en/?labs.20161013>

See also: 🗝️

Entry

Created: 03/30/2026 09:07 PM

Changes: 03/30/2026 09:07 PM (56)

Complete: 🔍

Submitter: [dyh18](#)

Cache ID: 135:B47:179

Submit

Accepted

- [Submit #780379](#): SourceCodester Teacher Record System 1.0 SQL Injection (by [dyh18](#))

Discussion

No comments yet. Languages: en.

Please log in to comment.