VDB-307332 · CVE-2025-4241 · GCVE-100-307332

PHPGURUKUL TEACHER SUBJECT ALLOCATION MANAGEMENT SYSTEM 1.0 /ADMIN/SEARCH.PHP SEARCHDATA SQL INJECTION

A vulnerability classified as critical has been found in PHPGurukul Teacher Subject Allocation Management System 1.0. Affected is an unknown code of the file */admin/search.php*. The manipulation of the argument `searchdata` with an unknown input leads to a sql injection vulnerability. CWE is classifying the issue as 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. This is going to have an impact on confidentiality, integrity, and availability.

The advisory is shared for download at github.com. This vulnerability is traded as CVE-2025-4241. The exploitability is told to be easy. It is possible to launch the attack remotely. The exploitation doesn't require any form of authentication. Technical details and a public exploit are known. The MITRE ATT&CK project declares the attack technique as T1505.

The exploit is shared for download at github.com. It is declared as proof-of-concept. By approaching the search of inurl:admin/search.php it is possible to find vulnerable targets with Google Hacking.

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

The entries VDB-207301, VDB-257610, VDB-257612 and VDB-258684 are pretty similar.

Product

Vendor

- PHPGurukul

Name

- Teacher Subject Allocation Management System

Version

- 1.0

License

- free

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA CVSS-B Score: 🔒
CNA CVSS-BT Score: 🔒
CNA Vector: 🔒

CVSSv3

VulDB Meta Base Score: 7.3
VulDB Meta Temp Score: 6.9

VulDB Base Score: 7.3
VulDB Temp Score: 6.6
VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA Base Score: 7.3
CNA Vector: 🔒

CVSSv2

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

Exploiting

Class: Sql injection
CWE: CWE-89 / CWE-74 / CWE-707
CAPEC: 🔒

ATT&CK: 🔒

Local: No
Remote: Yes

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

Threat Intelligence

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

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

05/02/2025		Advisory disclosed
05/02/2025	+0 days	VulDB entry created
05/03/2025	+1 days	VulDB entry last update

Sources

Vendor: phpgurukul.com

Advisory: github.com
Status: Not defined

CVE: CVE-2025-4241 (🔒)
GCVE (CVE): GCVE-0-2025-4241
GCVE (VulDB): GCVE-100-307332
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 05/02/2025 10:35 PM
Updated: 05/03/2025 08:35 PM
Changes: 05/02/2025 10:35 PM (55), 05/03/2025 08:35 PM (30)
Complete: 🔍
Submitter: bluechips
Cache ID: 5:A67:101

Submit

Accepted

- Submit #562452: phpgurukul Teacher Subject Allocation Management System V1.0 SQL Injection (by bluechips)

Discussion

No comments yet. Languages: en.

Please log in to comment.