



VDB-356294 · CVE-2026-5838 · EUVD-2026-20847

PHPGURUKUL NEWS PORTAL PROJECT 4.1 /ADMIN/ADD-SUBADMINS.PHP SADMINUSERNAME SQL INJECTION

CVSS Meta Temp Score ⓘ

4.3

Current Exploit Price (≈) ⓘ

\$0-\$5k

CTI Interest Score ⓘ

2.47-

Summary

A vulnerability categorized as **critical** has been discovered in [PHPGurukul News Portal Project 4.1](#). This issue affects some unknown processing of the file `/admin/add-subadmins.php`. Such manipulation of the argument `sadminusername` leads to sql injection. This vulnerability is traded as [CVE-2026-5838](#). The attack may be launched remotely. Furthermore, there is an exploit available.

Details

A vulnerability, which was classified as critical, has been found in [PHPGurukul News Portal Project 4.1](#). Affected by this issue is an unknown functionality of the file `/admin/add-subadmins.php`. The manipulation of the argument `sadminusername` with an unknown input leads to a sql injection vulnerability. Using CWE to declare the problem leads to [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. Impacted is confidentiality, integrity, and availability.

The advisory is available at [github.com](#). This vulnerability is handled as [CVE-2026-5838](#). The exploitation is known to be easy. The attack may be launched remotely. Additional levels of successful authentication are needed for exploitation. Technical details as well as a public exploit are known. This vulnerability is assigned to [T1505](#) by the MITRE ATT&CK project.

The exploit is available at [github.com](#). It is declared as proof-of-concept. By approaching the search of `inurl:admin/add-subadmins.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 vulnerability is also documented in the vulnerability database at EUVD ([EUVD-2026-20847](#)).

Product

Type

- [Project Management Software](#)

Vendor

- [PHPGurukul](#)

Name

- [News Portal Project](#)

Version

- [4.1](#)

License

- [free](#)

Website

- Vendor: <https://phpgurukul.com/>


CPE 2.3

- 

CPE 2.2

- 

CVSSv4

VuIDB Vector: 

VuIDB Reliability: 

CVSSv3

VuIDB Meta Base Score: 4.7

VuIDB Meta Temp Score: 4.3

VuIDB Base Score: 4.7

VuIDB Temp Score: 4.3

VuIDB Vector: 

VuIDB 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: 🔒

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

04/08/2026		Advisory disclosed
04/08/2026	+0 days	VulDB entry created
04/09/2026	+1 days	VulDB entry last update

Sources

Vendor: phpgurukul.com

Advisory: github.com

Status: Not defined

CVE: [CVE-2026-5838](#) (🔒)

GCVE (CVE): [GCVE-0-2026-5838](#)

GCVE (VulDB): [GCVE-100-356294](#)

EUVD: 🔒

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

Entry

Created: 04/08/2026 07:37 PM

Updated: 04/09/2026 07:44 AM

Changes: 04/08/2026 07:37 PM (56), 04/09/2026 07:44 AM (1)

Complete: 🔍

Cache ID: 20:C41:179

Submit

Accepted

- [Submit #789908](#): PHPGurukul News Portal Project 4.1 SQL Injection (by github.com)

Discussion

No comments yet. Languages: en.

Please log in to comment.