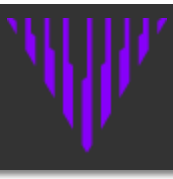

VDB-355431 · CVE-2026-5643 · GCVE-100-355431

CYBER-III STUDENT-MANAGEMENT-SYSTEM UP TO 1A938FA61E9F735078E9B291D2E6215B4942AF3F ADMIN ADD ENDPOINT NOTICE.PHP $_SERVER['PHP_SELF'] CROSS SITE SCRIPTING

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
2.2	$0-$5k	2.16-

Summary

A vulnerability classified as problematic has been found in Cyber-III Student-Management-System up to 1a938fa61e9f735078e9b291d2e6215b4942af3f. Affected is an unknown function of the file */admin/Add%20notice/notice.php* of the component *Admin Add Endpoint*. Performing a manipulation of the argument *$_SERVER['PHP_SELF']* results in cross site scripting. This vulnerability is identified as CVE-2026-5643. The attack can be initiated remotely. Additionally, an exploit exists. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet.

Details

A vulnerability, which was classified as problematic, was found in Cyber-III Student-Management-System up to 1a938fa61e9f735078e9b291d2e6215b4942af3f. This affects some unknown processing of the file */admin/Add%20notice/notice.php* of the component *Admin Add Endpoint*. The manipulation of the argument `$_SERVER['PHP_SELF']` with an unknown input leads to a cross site scripting vulnerability. CWE is classifying the issue as CWE-79. The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users. This is going to have an impact on integrity.

It is possible to read the advisory at github.com. This vulnerability is uniquely identified as CVE-2026-5643. The exploitability is told to be easy. It is possible to initiate the attack remotely. The exploitation needs additional levels of successful authentication. It demands that the victim is doing some kind of user interaction. Technical details and a public exploit are known. The attack technique deployed by this issue is T1059.007 according to MITRE ATT&CK.

The exploit is shared for download at github.com. It is declared as proof-of-concept. The project was informed of the problem early through an issue report but has not responded yet. By approaching the search of inurl:admin/Add%20notice/notice.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.

Product

Vendor

- Cyber-III

Name

- Student-Management-System

Version

- 1a938fa61e9f735078e9b291d2e6215b4942af3f

Website

- Product: https://github.com/Cyber-III/Student-Management-System/

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 2.4
VulDB Meta Temp Score: 2.2

VulDB Base Score: 2.4
VulDB Temp Score: 2.2

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

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

Exploiting

Class: Cross site scripting
CWE: CWE-79 / CWE-94 / CWE-74
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

04/05/2026		Advisory disclosed
04/05/2026	+0 days	VulDB entry created
04/05/2026	+0 days	VulDB entry last update

Sources

Product: github.com

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5643 (🔒)
GCVE (CVE): GCVE-0-2026-5643
GCVE (VulDB): GCVE-100-355431
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 04/05/2026 10:41 PM
Changes: 04/05/2026 10:41 PM (58)
Complete: 🔍
Submitter: springbot
Cache ID: 64:C90:179

Submit

Accepted

- Submit #785859: Cyber-III Student-Management-System 1.0 Insecure Direct Object Reference (by springbot)

Discussion

No comments yet. Languages: en.

Please log in to comment.