VDB-355432 · CVE-2026-5644 · ISSUE 238

CYBER-III STUDENT-MANAGEMENT-SYSTEM UP TO 1A938FA61E9F735078E9B291D2E6215B4942AF3F BATCH-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 was found in Cyber-III Student-Management-System up to 1a938fa61e9f735078e9b291d2e6215b4942af3f. Affected by this vulnerability is an unknown functionality of the file */admin/Add%20notice/batch-notice.php*. Executing a manipulation of the argument *$_SERVER['PHP_SELF']* can lead to cross site scripting. This vulnerability is tracked as CVE-2026-5644. The attack can be launched remotely. Moreover, an exploit is present. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The project was informed of the problem early through an issue report but has not responded yet.

Details

A vulnerability has been found in Cyber-III Student-Management-System up to 1a938fa61e9f735078e9b291d2e6215b4942af3f and classified as problematic. This vulnerability affects an unknown function of the file */admin/Add%20notice/batch-notice.php*. The manipulation of the argument `$_SERVER['PHP_SELF']` with an unknown input leads to a cross site scripting vulnerability. The CWE definition for the vulnerability is 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. As an impact it is known to affect integrity.

The advisory is shared for download at github.com. This vulnerability was named CVE-2026-5644. The exploitation appears to be easy. The attack can be initiated remotely. Additional levels of successful authentication are required for exploitation. Successful exploitation requires user interaction by the victim. Technical details and also a public exploit are known. The MITRE ATT&CK project declares the attack technique as T1059.007.

It is possible to download the exploit 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/batch-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: 238
Status: Not defined

CVE: CVE-2026-5644 (🔒)
GCVE (CVE): GCVE-0-2026-5644
GCVE (VulDB): GCVE-100-355432
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: Z3r0_0
Cache ID: 135:C1A:179

Submit

Accepted

- Submit #785867: Cyber-III Student-Management-System 1.0 XSS vulnerability (by Z3r0_0)

Discussion

No comments yet. Languages: en.

Please log in to comment.