VDB-355430 · CVE-2026-5642 · ISSUE 236

CYBER-III STUDENT-MANAGEMENT-SYSTEM UP TO 1A938FA61E9F735078E9B291D2E6215B4942AF3F HTTP POST REQUEST /VIVA/UPDATE.PHP NAME IMPROPER AUTHORIZATION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
6.6	$0-$5k	1.78-

Summary

A vulnerability described as critical has been identified in Cyber-III Student-Management-System up to 1a938fa61e9f735078e9b291d2e6215b4942af3f. This impacts an unknown function of the file */viva/update.php* of the component *HTTP POST Request Handler*. Such manipulation of the argument *Name* leads to improper authorization. This vulnerability is referenced as CVE-2026-5642. It is possible to launch the attack remotely. Furthermore, an exploit is available. This product takes the approach of rolling releases to provide continious delivery. Therefore, version details for affected and updated releases are not 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 critical, has been found in Cyber-III Student-Management-System up to 1a938fa61e9f735078e9b291d2e6215b4942af3f. Affected by this issue is an unknown code block of the file */viva/update.php* of the component *HTTP POST Request Handler*. The manipulation of the argument `name` with an unknown input leads to a improper authorization vulnerability. Using CWE to declare the problem leads to CWE-285. The product does not perform or incorrectly performs an authorization check when an actor attempts to access a resource or perform an action. Impacted is confidentiality, integrity, and availability.

The advisory is available at github.com. This vulnerability is handled as CVE-2026-5642. The exploitation is known to be easy. The attack may be launched remotely. No form of authentication is required for exploitation. Technical details as well as a public exploit are known. This vulnerability is assigned to T1548.002 by the MITRE ATT&CK project.

The exploit is available 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:viva/update.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.

Similar entries are available at VDB-185300 and VDB-189788.

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: 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: Improper authorization
CWE: CWE-285 / CWE-266
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: 236
Status: Not defined

CVE: CVE-2026-5642 (🔒)
GCVE (CVE): GCVE-0-2026-5642
GCVE (VulDB): GCVE-100-355430
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/05/2026 10:41 PM
Changes: 04/05/2026 10:41 PM (59)
Complete: 🔍
Submitter: xhh400plus
Cache ID: 128:E81:179

Submit

Accepted

- Submit #785857: Cyber-III Student-Management-System 1.0 Insecure Direct Object Reference (by xhh400plus)

Discussion

No comments yet. Languages: en.

Please log in to comment.