VDB-356609 · CVE-2026-6033 · GCVE-100-356609

CODEASTRO ONLINE CLASSROOM 1.0 UPDATEDETAILSFROMSTUDENT.PHP? ENO=146891650 FNAME SQL INJECTION

CVSS Meta Temp Score | Current Exploit Price (≈) | CTI Interest Score

5.7 | $0-$5k | 1.35

Summary

A vulnerability, which was classified as critical, has been found in CodeAstro Online Classroom 1.0. Affected by this vulnerability is an unknown functionality of the file */updatedetailsfromstudent.php?eno=146891650*. The manipulation of the argument *fname* leads to sql injection. This vulnerability is traded as CVE-2026-6033. It is possible to initiate the attack remotely. Furthermore, there is an exploit available.

Details

A vulnerability, which was classified as critical, has been found in CodeAstro Online Classroom 1.0. This issue affects an unknown functionality of the file */updatedetailsfromstudent.php?eno=146891650*. The manipulation of the argument `fname` 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 shared at github.com. The identification of this vulnerability is CVE-2026-6033. The exploitation is known to be easy. The attack may be initiated remotely. Technical details as well as a public exploit are known. MITRE ATT&CK project uses the attack technique T1505 for this issue.

The exploit is available at github.com. It is declared as proof-of-concept.

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

The entries VDB-319340, VDB-321788, VDB-323843 and VDB-333347 are related to this item.

Product

Vendor

- CodeAstro

Name

- Online Classroom

Version

- 1.0

Website

- Vendor: https://codeastro.com/

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 6.3
VulDB Meta Temp Score: 5.7

VulDB Base Score: 6.3
VulDB Temp Score: 5.7
VulDB Vector: 🔒
VulDB 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: 🔒
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

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

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

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

Sources

Vendor: codeastro.com

Advisory: github.com
Status: Not defined

CVE: CVE-2026-6033 (🔒)
GCVE (CVE): GCVE-0-2026-6033
GCVE (VulDB): GCVE-100-356609
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/09/2026 06:15 PM
Changes: 04/09/2026 06:15 PM (55)
Complete: 🔍
Submitter: yu_ji
Cache ID: 52:E84:179

Submit

Accepted

- Submit #795773: codeastro Online Classroom V1.0 SQL Injection (by yu_ji)

Discussion

No comments yet. Languages: en.

Please log in to comment.