



VDB-355350 · CVE-2026-5580 · GCVE-100-355350

CODEASTRO ONLINE CLASSROOM 1.0 PARAMETER ADDVIDEOS.PHP VIDEOTITLE SQL INJECTION

CVSS Meta Temp Score ⓘ

5.7

Current Exploit Price (≈) ⓘ

\$0-\$5k

CTI Interest Score ⓘ

1.31

Summary

A vulnerability, which was classified as **critical**, was found in [CodeAstro Online Classroom 1.0](#). The affected element is an unknown function of the file `/OnlineClassroom/addvideos.php` of the component *Parameter Handler*. The manipulation of the argument `videotitle` results in sql injection. This vulnerability is known as [CVE-2026-5580](#). It is possible to launch the attack remotely. Furthermore, an exploit is available.

Details

A vulnerability, which was classified as **critical**, was found in [CodeAstro Online Classroom 1.0](#). Affected is some unknown functionality of the file `/OnlineClassroom/addvideos.php` of the component *Parameter Handler*. The manipulation of the argument `videotitle` with an unknown input leads to a sql injection vulnerability. CWE is classifying the issue as [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. This is going to have an impact on confidentiality, integrity, and availability.

The advisory is available at [github.com](#). This vulnerability is traded as [CVE-2026-5580](#). The exploitability is told to be easy. It is possible to launch the attack remotely. Technical details and a public exploit are known. This vulnerability is assigned to **T1505** by the MITRE ATT&CK project.

The exploit is shared for download at [github.com](#). It is declared as proof-of-concept. By approaching the search of `inurl:OnlineClassroom/addvideos.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

- [CodeAstro](#)

Name

- [Online Classroom](#)

Version

- [1.0](#)

Website

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


CPE 2.3

- 

CPE 2.2

- 

CVSSv4

VuIDB Vector: 

VuIDB Reliability: 

CVSSv3

VuIDB Meta Base Score: 6.3

VuIDB Meta Temp Score: 5.7

VuIDB Base Score: 6.3

VuIDB Temp Score: 5.7

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

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

Sources

Vendor: codeastro.com

Advisory: github.com

Status: Not defined

CVE: [CVE-2026-5580](#) (🗝️)

GCVE (CVE): [GCVE-0-2026-5580](#)

GCVE (VulDB): [GCVE-100-355350](#)

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

Entry

Created: 04/04/2026 05:07 PM

Changes: 04/04/2026 05:07 PM (56)

Complete: 🔍

Submitter: [zws58](#)

Cache ID: 4:0E7:179

Submit

Accepted

- [Submit #783753](#): codeastro Online Classroom V1.0 SQL Injection (by zws58)

Discussion

No comments yet. Languages: en.

Please log in to comment.