VDB-307360 · CVE-2025-4256 · ISSUE 25

SEACMS 13.2 /ADMIN_PAYLOG.PHP CSTATUS CROSS SITE SCRIPTING

A vulnerability classified as problematic was found in SeaCMS 13.2. This vulnerability affects an unknown code of the file */admin_paylog.php*. The manipulation of the argument `cstatus` 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-2025-4256. The exploitation appears to be easy. The attack can be initiated remotely. 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. By approaching the search of inurl:admin_paylog.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 entry is available at VDB-307361.

Product

Type

- Content Management System

Name

- SeaCMS

Version

- 13.2

License

- free

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA CVSS-B Score: 🔒
CNA CVSS-BT Score: 🔒
CNA Vector: 🔒

CVSSv3

VulDB Meta Base Score: 3.5
VulDB Meta Temp Score: 3.3

VulDB Base Score: 3.5
VulDB Temp Score: 3.2
VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA Base Score: 3.5
CNA Vector: 🔒

CVSSv2

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

Exploiting

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

ATT&CK: 🔒

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

05/04/2025		Advisory disclosed
05/04/2025	+0 days	VulDB entry created
05/05/2025	+1 days	VulDB entry last update

Sources

Advisory: 25
Status: Not defined

CVE: CVE-2025-4256 (🔒)
GCVE (CVE): GCVE-0-2025-4256
GCVE (VulDB): GCVE-100-307360
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 05/04/2025 09:04 AM
Updated: 05/05/2025 01:21 PM
Changes: 05/04/2025 09:04 AM (56), 05/05/2025 05:49 AM (30), 05/05/2025 01:21 PM (1)
Complete: 🔍
Submitter: zonesec
Cache ID: 5:0B7:101

Submit

Accepted

- Submit #562718: GitHub seccms v13.2 Cross Site Scripting (by zonesec)

Discussion

No comments yet. Languages: en.

Please log in to comment.