



VDB-307361 · CVE-2025-4257 · ISSUE 26

SEACMS 13.2 /ADMIN_PAY.PHP CSTATUS CROSS SITE SCRIPTING

A vulnerability, which was classified as problematic, has been found in SeaCMS 13.2. This issue affects an unknown code block of the file `/admin_pay.php`. The manipulation of the argument `cstatus` with an unknown input leads to a cross site scripting vulnerability. Using CWE to declare the problem leads to 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. Impacted is integrity.

The advisory is shared at github.com. The identification of this vulnerability is CVE-2025-4257. The exploitation is known to be easy. The attack may be initiated remotely. It demands that the victim is doing some kind of user interaction. Technical details as well as a public exploit are known. MITRE ATT&CK project uses the attack technique T1059.007 for this issue.

The exploit is available at github.com. It is declared as proof-of-concept. By approaching the search of `inurl:admin_pay.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.

Entry connected to this vulnerability is available at VDB-307360.

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

CVSSv2 Base Score	CVSSv2 Temp Score	CVSSv2 Base Score	CVSSv2 Temp Score	CVSSv2 Base Score	CVSSv2 Temp Score
3.5	3.2	3.5	3.2	3.5	3.2
3.5	3.2	3.5	3.2	3.5	3.2
3.5	3.2	3.5	3.2	3.5	3.2

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: 26
Status: Not defined

CVE: CVE-2025-4257 (🔒)
GCVE (CVE): GCVE-0-2025-4257
GCVE (VulDB): GCVE-100-307361
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: 5:791:101

Submit

Accepted

- Submit #562719: GitHub seacms v13.2 Cross Site Scripting (by zonesec)

Discussion

No comments yet. Languages: en.

Please log in to comment.