VDB-356260 · CVE-2026-5812 · GCVE-100-356260

SOURCECODESTER PHARMACY PRODUCT MANAGEMENT SYSTEM 1.0 POST PARAMETER ADD-SALES.PHP TXTQTY LOGIC ERROR

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

4.9 | $0-$5k | 1.68

Summary

A vulnerability, which was classified as critical, was found in SourceCodester Pharmacy Product Management System 1.0. This vulnerability affects unknown code of the file *add-sales.php* of the component *POST Parameter Handler*. Executing a manipulation of the argument *txtqty* can lead to logic error. This vulnerability is registered as CVE-2026-5812. It is possible to launch the attack remotely. Furthermore, an exploit is available.

Details

A vulnerability has been found in SourceCodester Pharmacy Product Management System 1.0 and classified as critical. This vulnerability affects some unknown functionality of the file *add-sales.php* of the component *POST Parameter Handler*. The manipulation of the argument `txtqty` with an unknown input leads to a logic error vulnerability. The CWE definition for the vulnerability is CWE-840. As an impact it is known to affect integrity, and availability.

The advisory is shared for download at github.com. This vulnerability was named CVE-2026-5812. The exploitation appears to be easy. The attack can be initiated remotely. Technical details and also a public exploit are known.

It is possible to download the exploit at github.com. It is declared as proof-of-concept. By approaching the search of inurl:add-sales.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

- SourceCodester

Name

- Pharmacy Product Management System

Version

- 1.0

License

- free

Website

- Vendor: https://www.sourcecodester.com/

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 5.4
VulDB Meta Temp Score: 4.9

VulDB Base Score: 5.4
VulDB Temp Score: 4.9
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

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

Exploiting

Class: Logic error
CWE: CWE-840
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

04/08/2026		Advisory disclosed
04/08/2026	+0 days	VulDB entry created
04/08/2026	+0 days	VulDB entry last update

Sources

Vendor: sourcecodester.com

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5812 (🔒)
GCVE (CVE): GCVE-0-2026-5812
GCVE (VulDB): GCVE-100-356260
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 04/08/2026 05:27 PM
Changes: 04/08/2026 05:27 PM (56)
Complete: 🔍
Submitter: FuKun
Cache ID: 74:8AB:179

Submit

Accepted

- Submit #787680: SourceCodester Pharmacy Product Management System 1.0 Business Logic Errors (by github.com)

Discussion

No comments yet. Languages: en.

Please log in to comment.