VDB-354656 · CVE-2026-5325 · GCVE-100-354656

SOURCECODESTER SIMPLE CUSTOMER RELATIONSHIP MANAGEMENT SYSTEM 1.0 CREATE TICKET /CREATE-TICKET.PHP DESCRIPTION CROSS SITE SCRIPTING

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
3.2	$0-$5k	1.38-

Summary

A vulnerability categorized as problematic has been discovered in SourceCodester Simple Customer Relationship Management System 1.0. Impacted is an unknown function of the file */create-ticket.php* of the component *Create Ticket*. Such manipulation of the argument *Description* leads to cross site scripting. This vulnerability is documented as CVE-2026-5325. The attack can be executed remotely. Additionally, an exploit exists.

Details

A vulnerability, which was classified as problematic, has been found in SourceCodester Simple Customer Relationship Management System 1.0. Affected by this issue is an unknown functionality of the file */create-ticket.php* of the component *Create Ticket*. The manipulation of the argument `description` 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 for download at medium.com. This vulnerability is handled as CVE-2026-5325. The exploitation is known to be easy. The attack may be launched remotely. Successful exploitation requires user interaction by the victim. Technical details as well as a public exploit are known. The MITRE ATT&CK project declares the attack technique as T1059.007.

The exploit is available at medium.com. It is declared as proof-of-concept. By approaching the search of inurl:create-ticket.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-324785.

Product

Vendor

- SourceCodester

Name

- Simple Customer Relationship Management System

Version

- 1.0

License

- free

Website

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

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

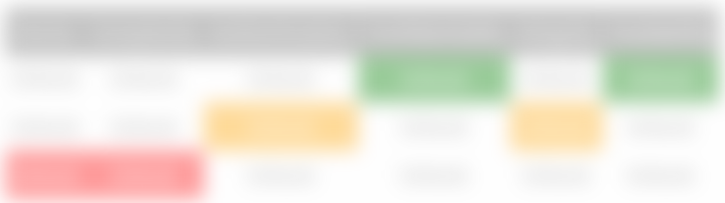
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 3.5
VulDB Meta Temp Score: 3.2

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

CVSSv2



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

Exploiting

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

04/01/2026		Advisory disclosed
04/01/2026	+0 days	VulDB entry created
04/01/2026	+0 days	VulDB entry last update

Sources

Vendor: sourcecodester.com

Advisory: medium.com
Status: Not defined

CVE: CVE-2026-5325 (🔒)
GCVE (CVE): GCVE-0-2026-5325
GCVE (VulDB): GCVE-100-354656
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/01/2026 03:20 PM
Changes: 04/01/2026 03:20 PM (56)
Complete: 🔍
Submitter: Hemant Raj Bhati
Cache ID: 40:1FB:179

Submit

Accepted

- Submit #780766: SourceCodester Simple Customer Relationship Management (CRM) System 1.0 Cross Site Scripting (by Hemant Raj Bhati)

Discussion

No comments yet. Languages: en.

Please log in to comment.