



VDB-205300 · CVE-2022-2577

# SOURCECODESTER GARAGE MANAGEMENT SYSTEM 1.0 /EDITUSER.PHP ID SQL INJECTION

CVSS Meta Temp Score (?)

6.9

Current Exploit Price (≈) (?)

\$0-\$5k

CTI Interest Score (?)

0.10

A vulnerability classified as critical was found in SourceCodester Garage Management System 1.0. This vulnerability affects an unknown code of the file `/edituser.php`. The manipulation of the argument `id` with the input value `-2'%20UNION%20select%2011,user(),333,444--+` 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 07/29/2022. The advisory is shared for download at [github.com](https://github.com). This vulnerability was named CVE-2022-2577. 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](https://github.com). By approaching the search of `inurl:edituser.php` it is possible to find vulnerable targets with Google Hacking.

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: 7.1  
VulDB Meta Temp Score: 6.9




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

NVD Base Score: 8.8  
NVD Vector: 

CNA Base Score: 6.3  
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

07/29/2022		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](https://github.com)  
Status: Not defined

CVE: CVE-2022-2577 (  )  
scip Labs: <https://www.scip.ch/en/?labs.20161013>

## Entry

Created: 07/29/2022 03:12 PM

Updated: 08/28/2022 02:47 PM

Changes: 07/29/2022 03:12 PM (42), 08/28/2022 02:41 PM (2), 08/28/2022 02:45 PM (21), 08/28/2022 02:47 PM (1)

Complete: 

Submitter: webray.com.cn

## Discussion

No comments yet. Languages: en.

Please log in to comment.