



VDB-356619 · CVE-2026-6038 · GCVE-100-356619

# CODE-PROJECTS VEHICLE SHOWROOM MANAGEMENT SYSTEM 1.0 REGISTERCUSTOMERFUNCTION.PHP BRANCH\_ID SQL INJECTION

CVSS Meta Temp Score ⓘ

6.6

Current Exploit Price (≈) ⓘ

\$0-\$5k

CTI Interest Score ⓘ

2.25-

## Summary

A vulnerability marked as [critical](#) has been reported in [code-projects Vehicle Showroom Management System 1.0](#). Affected is an unknown function of the file `/util/RegisterCustomerFunction.php`. Performing a manipulation of the argument `BRANCH_ID` results in sql injection. This vulnerability is cataloged as [CVE-2026-6038](#). It is possible to initiate the attack remotely. Furthermore, there is an exploit available.

## Details

A vulnerability, which was classified as critical, was found in [code-projects Vehicle Showroom Management System 1.0](#). This affects an unknown code of the file `/util/RegisterCustomerFunction.php`. The manipulation of the argument `BRANCH_ID` with an unknown input leads to a sql injection vulnerability. CWE is classifying the issue as [CWE-89](#). The product 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. This is going to have an impact on confidentiality, integrity, and availability.

It is possible to read the advisory at [github.com](#). This vulnerability is uniquely identified as [CVE-2026-6038](#). The exploitability is told to be easy. It is possible to initiate the attack remotely. No form of authentication is needed for exploitation. Technical details and a public exploit are known. The attack technique deployed by this issue is [T1505](#) according to MITRE ATT&CK.

The exploit is shared for download at [github.com](#). It is declared as proof-of-concept. By approaching the search of `inurl:util/RegisterCustomerFunction.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.

The entries [VDB-356615](#), [VDB-356616](#) and [VDB-356618](#) are related to this item.

## Product

### Type

- [Project Management Software](#)

### Vendor

- [code-projects](#)

### Name

- [Vehicle Showroom Management System](#)

### Version

- [1.0](#)

### License

- [free](#)

### Website

- Vendor: <https://code-projects.org/>

## CPE 2.3

- 

## CPE 2.2

- 

## CVSSv4

VuIDB Vector: 

VuIDB Reliability: 

## CVSSv3

VuIDB Meta Base Score: 7.3

VuIDB Meta Temp Score: 6.6

VuIDB Base Score: 7.3

VuIDB Temp Score: 6.6

VuIDB Vector: 

VuIDB Reliability: 

## CVSSv2

VulDB Base Score: 🔒

VulDB Temp Score: 🔒

VulDB Reliability: 🔍

## Exploiting

Class: Sql injection

CWE: [CWE-89](#) / [CWE-74](#) / [CWE-707](#)

CAPEC: 🔒

ATT&CK: 🔒

Physical: No

Local: No

Remote: Yes

Availability: 🔒

Access: Public

Status: Proof-of-Concept

Download: 🔒

Google Hack: 🔒

Price Prediction: 🔍

Current Price Estimation: 🔒

## Threat Intelligence

Interest: 🔍

Active Actors: 🔍

Active APT Groups: 🔍

## Countermeasures

**Recommended:** no mitigation known

**Status:** 🔍

**0-Day Time:** 🔒

## Timeline

04/09/2026		Advisory disclosed
04/09/2026	+0 days	VulDB entry created
04/09/2026	+0 days	VulDB entry last update

## Sources

**Vendor:** [code-projects.org](https://code-projects.org)

**Advisory:** [github.com](https://github.com)

**Status:** Not defined

**CVE:** [CVE-2026-6038](#) (🔒)

**GCVE (CVE):** [GCVE-0-2026-6038](#)

**GCVE (VulDB):** [GCVE-100-356619](#)

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

**See also:** 🔒

## Entry

**Created:** 04/09/2026 06:28 PM

**Changes:** 04/09/2026 06:28 PM (23), 04/09/2026 06:29 PM (33)

**Complete:** 🔍

**Submitter:** 125hzb

**Cache ID:** 20:6D4:179

## Submit

**Accepted**

- [Submit #796281](#): code-projects Vehicle Showroom Management System V1.0 SQL injection (by 125hzb)

## Discussion

No comments yet. Languages: en.

Please log in to comment.