



VDB-357033 · CVE-2026-6153 · SUBMIT #357033

CODE-PROJECTS VEHICLE SHOWROOM MANAGEMENT SYSTEM 1.0 STAFFDETAILSFUNCTION.PHP STAFF_ID SQL INJECTION

CVSS Meta Temp Score ⓘ

6.6

Current Exploit Price (≈) ⓘ

\$0-\$5k

CTI Interest Score ⓘ

2.47

Summary

A vulnerability was found in [code-projects Vehicle Showroom Management System 1.0](#). It has been classified as **critical**. The affected element is an unknown function of the file `/util/StaffDetailsFunction.php`. Performing a manipulation of the argument `STAFF_ID` results in sql injection. This vulnerability was named [CVE-2026-6153](#). The attack may be initiated remotely. In addition, an exploit is 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 block of the file `/util/StaffDetailsFunction.php`. The manipulation of the argument `STAFF_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.

The advisory is shared at [github.com](#). This vulnerability is uniquely identified as [CVE-2026-6153](#). 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. MITRE ATT&CK project uses the attack technique [T1505](#) for this issue.

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

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

VulDB Vector: 

VulDB Reliability: 

CVSSv3

VulDB Meta Base Score: 7.3

VulDB Meta Temp Score: 6.6

VulDB Base Score: 7.3

VulDB Temp Score: 6.6

VulDB Vector: 

VulDB 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

04/12/2026		Advisory disclosed
04/12/2026	+0 days	VulDB entry created
04/12/2026	+0 days	VulDB entry last update

Sources

Vendor: code-projects.org

Advisory: github.com

Status: Not defined

CVE: [CVE-2026-6153](#) (🗝️)

GCVE (CVE): [GCVE-0-2026-6153](#)

GCVE (VulDB): [GCVE-100-357033](#)

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

Entry

Created: 04/12/2026 08:05 PM

Changes: 04/12/2026 08:05 PM (56)

Complete: 🔍

Submitter: [huahuan](#)

Cache ID: 48:2BA:179

Submit

Accepted

- [Submit #796315](#): code-projects Vehicle Showroom Management System V1.0 SQL injection (by huahuan)

Discussion

No comments yet. Languages: en.

[Please log in to comment.](#)