



VDB-356616 · CVE-2026-6035 · GCVE-100-356616

CODE-PROJECTS VEHICLE SHOWROOM MANAGEMENT SYSTEM 1.0 SERVICEANDSALESREPORT.PHP BRANCH_ID CROSS SITE SCRIPTING

CVSS Meta Temp Score ⓘ

3.9

Current Exploit Price (≈) ⓘ

\$0-\$5k

CTI Interest Score ⓘ

2.26-

Summary

A vulnerability categorized as [problematic](#) has been discovered in [code-projects Vehicle Showroom Management System 1.0](#). The impacted element is an unknown function of the file `/BranchManagement/ServiceAndSalesReport.php`. The manipulation of the argument `BRANCH_ID` results in cross site scripting. This vulnerability is identified as [CVE-2026-6035](#). The attack can be executed remotely. Additionally, an exploit exists.

Details

A vulnerability classified as [problematic](#) has been found in [code-projects Vehicle Showroom Management System 1.0](#). Affected is an unknown functionality of the file `/BranchManagement/ServiceAndSalesReport.php`. The manipulation of the argument `BRANCH_ID` with an unknown input leads to a cross site scripting vulnerability. CWE is classifying the issue as [CWE-79](#). The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users. This is going to have an impact on integrity.

The advisory is shared for download at [github.com](#). This vulnerability is traded as [CVE-2026-6035](#). The exploitability is told to be easy. It is possible to launch the attack remotely. The exploitation doesn't require any form of authentication. Successful exploitation requires user interaction by the victim. Technical details and a public exploit are known. The MITRE ATT&CK project declares the attack technique as [T1059.007](#).

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

Entries connected to this vulnerability are available at [VDB-356615](#), [VDB-356618](#) and [VDB-356619](#).

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: 4.3

VuIDB Meta Temp Score: 3.9

VuIDB Base Score: 4.3

VuIDB Temp Score: 3.9

VuIDB Vector: 

VuIDB Reliability: 

CVSSv2

VulDB Base Score: 🔒

VulDB Temp Score: 🔒

VulDB Reliability: 🔍

Exploiting

Class: Cross site scripting

CWE: [CWE-79](#) / [CWE-94](#) / [CWE-74](#)

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

Advisory: github.com

Status: Not defined

CVE: [CVE-2026-6035](#) (🔒)

GCVE (CVE): [GCVE-0-2026-6035](#)

GCVE (VulDB): [GCVE-100-356616](#)

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

See also: 🔒

Entry

Created: 04/09/2026 06:27 PM

Changes: 04/09/2026 06:27 PM (56)

Complete: 🔍

Submitter: [tnn2026](#)

Cache ID: 172:D0F:179

Submit

Accepted

- [Submit #796200](#): code-projects Vehicle Showroom Management System V1.0 Cross Site Scripting (by tnn2026)

Discussion

No comments yet. Languages: en.

Please log in to comment.