



VDB-355293 · CVE-2026-5540 · GCVE-100-355293

CODE-PROJECTS SIMPLE LAUNDRY SYSTEM 1.0 PARAMETER /MODIFYMEMBER.PHP FIRSTNAME SQL INJECTION

CVSS Meta Temp Score

6.6

Current Exploit Price (€)

\$0-\$5k

CTI Interest Score

3.15-

Summary

A vulnerability, which was classified as [critical](#), has been found in [code-projects Simple Laundry System 1.0](#). This issue affects some unknown processing of the file `/modifymember.php` of the component `Parameter Handler`. Performing a manipulation of the argument `firstName` results in sql injection. This vulnerability was named [CVE-2026-5540](#). The attack may be initiated remotely. In addition, an exploit is available.

Details

A vulnerability classified as critical has been found in [code-projects Simple Laundry System 1.0](#). This affects an unknown functionality of the file `/modifymember.php` of the component `Parameter Handler`. The manipulation of the argument `firstName` 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-2026-5540](#). 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:modifymember.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.

See [VDB-355292](#) for similar entry.

Product

Type

- [Project Management Software](#)

Vendor

- [code-projects](#)

Name

- [Simple Laundry 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

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

Sources

Vendor: code-projects.org

Advisory: github.com

Status: Not defined

CVE: [CVE-2026-5540](#) (🔒)

GCVE (CVE): [GCVE-0-2026-5540](#)

GCVE (VulDB): [GCVE-100-355293](#)

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

See also: 🔒

Entry

Created: 04/04/2026 08:52 AM

Changes: 04/04/2026 08:52 AM (57)

Complete: 🔍

Submitter: [Weining Xiao](#)

Cache ID: 68:737:179

Submit

Accepted

- [Submit #782222](#): code-projects Simple Laundry System V1.0 SQL injection (by Weining Xiao)

Discussion

No comments yet. Languages: en.

Please log in to comment.