



VDB-355292 · CVE-2026-5539 · GCVE-100-355292

# CODE-PROJECTS SIMPLE LAUNDRY SYSTEM 1.0 PARAMETER /MODIFYMEMBER.PHP FIRSTNAME CROSS SITE SCRIPTING

CVSS Meta Temp Score

3.9

Current Exploit Price (≈)

\$0-\$5k

CTI Interest Score

2.50-

## Summary

A vulnerability classified as **problematic** was found in [code-projects Simple Laundry System 1.0](#). This vulnerability affects unknown code of the file `/modifymember.php` of the component *Parameter Handler*. Such manipulation of the argument `firstName` leads to cross site scripting. This vulnerability is uniquely identified as [CVE-2026-5539](#). The attack can be launched remotely. Moreover, an exploit is present.

## Details

A vulnerability was found in [code-projects Simple Laundry System 1.0](#). It has been rated as **problematic**. Affected by this issue is an unknown function of the file `/modifymember.php` of the component *Parameter Handler*. The manipulation of the argument `firstName` with an unknown input leads to a cross site scripting vulnerability. Using CWE to declare the problem leads to [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. Impacted is integrity.

The advisory is shared for download at [github.com](#). This vulnerability is handled as [CVE-2026-5539](#). The exploitation is known to be easy. The attack may be launched remotely. No form of authentication is required for exploitation. Successful exploitation requires user interaction by the victim. Technical details as well as a public exploit are known. The MITRE ATT&CK project declares the attack technique as [T1059.007](#).

The exploit is available 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.

The entry [VDB-355293](#) is pretty similar.

## 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

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

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

## Sources

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

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

**Status:** Not defined

**CVE:** [CVE-2026-5539](#) (🗝️)

**GCVE (CVE):** [GCVE-0-2026-5539](#)

**GCVE (VulDB):** [GCVE-100-355292](#)

**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:** 52:D09:179

## Submit

### Accepted

- [Submit #782221](#): code-projects Simple Laundry System V1.0 cross site scripting (by Weining Xiao)

## Discussion

No comments yet. Languages: en.

Please log in to comment.