



VDB-355295 · CVE-2026-5542 · GCVE-100-355295

CODE-PROJECTS SIMPLE LAUNDRY SYSTEM 1.0 PARAMETER /MODSTAFFINFO.PHP USERID CROSS SITE SCRIPTING

CVSS Meta Temp Score ⓘ

3.9

Current Exploit Price (≈) ⓘ

\$0-\$5k

CTI Interest Score ⓘ

3.63-

Summary

A vulnerability has been found in [code-projects Simple Laundry System 1.0](#) and classified as **problematic**. The affected element is an unknown function of the file `/modstaffinfo.php` of the component *Parameter Handler*. The manipulation of the argument `userid` leads to cross site scripting. This vulnerability is referenced as [CVE-2026-5542](#). Remote exploitation of the attack is possible. Furthermore, an exploit is available.

Details

A vulnerability, which was classified as **problematic**, has been found in [code-projects Simple Laundry System 1.0](#). This issue affects an unknown part of the file `/modstaffinfo.php` of the component *Parameter Handler*. The manipulation of the argument `userid` 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.

It is possible to read the advisory at [github.com](#). The identification of this vulnerability is [CVE-2026-5542](#). The exploitation is known to be easy. The attack may be initiated remotely. No form of authentication is needed for a successful exploitation. It demands that the victim is doing some kind of user interaction. Technical details as well as a public exploit are known. The attack technique deployed by this issue is [T1059.007](#) according to MITRE ATT&CK.

The exploit is available at [github.com](#). It is declared as proof-of-concept. By approaching the search of `inurl:modstaffinfo.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.

Similar entry is available at [VDB-353659](#).

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

Advisory: github.com

Status: Not defined

CVE: [CVE-2026-5542](#) (🔒)

GCVE (CVE): [GCVE-0-2026-5542](#)

GCVE (VulDB): [GCVE-100-355295](#)

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: 57:356:179

Submit

Accepted

- [Submit #782224](#): code-projects Simple Laundry System V1.0 cross site scripting (by Weining Xiao)

Discussion

No comments yet. Languages: en.

Please log in to comment.