



VDB-356271 · CVE-2026-5824 · GCVE-100-356271

# CODE-PROJECTS SIMPLE LAUNDRY SYSTEM 1.0 /USERCHECKLOGIN.PHP USERID SQL INJECTION

CVSS Meta Temp Score

6.6

Current Exploit Price (≈)

\$0-\$5k

CTI Interest Score

1.12

## Summary

A vulnerability classified as **critical** has been found in [code-projects Simple Laundry System 1.0](#). This vulnerability affects unknown code of the file `/userchecklogin.php`. Performing a manipulation of the argument `userid` results in sql injection. This vulnerability is identified as [CVE-2026-5824](#). The attack can be initiated remotely. Additionally, an exploit exists.

## Details

A vulnerability was found in [code-projects Simple Laundry System 1.0](#). It has been classified as **critical**. This affects some unknown processing of the file `/userchecklogin.php`. The manipulation of the argument `userid` 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.

It is possible to read the advisory at [github.com](#). This vulnerability is uniquely identified as [CVE-2026-5824](#). 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. The attack technique deployed by this issue is [T1505](#) according to MITRE ATT&CK.

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

- [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: 7.3

VuIDB Meta Temp Score: 6.6

VuIDB Base Score: 7.3

VuIDB Temp Score: 6.6

VuIDB Vector: 

VuIDB 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

<b>04/08/2026</b>		Advisory disclosed
<b>04/08/2026</b>	+0 days	VulDB entry created
<b>04/08/2026</b>	+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-2026-5824](#) (🗝️)

**GCVE (CVE):** [GCVE-0-2026-5824](#)

**GCVE (VulDB):** [GCVE-100-356271](#)

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

## Entry

**Created:** 04/08/2026 06:54 PM

**Changes:** 04/08/2026 06:54 PM (56)

**Complete:** 🔍

**Submitter:** [christychen11](#)

**Cache ID:** 20:758:179

## Submit

**Accepted**

- [Submit #788302](#): code-projects Simple Laundry System V1.0 SQL injection (by christychen11)

## Discussion

No comments yet. Languages: en.

Please log in to comment.