VDB-355345 · CVE-2026-5575 · GCVE-100-355345

# SOURCECODESTER/JKEV RECORD MANAGEMENT SYSTEM 1.0 LOGIN INDEX.PHP USERNAME SQL INJECTION

| CVSS Meta Temp Score | Current Exploit Price (≈) | CTI Interest Score |
|---|---|---|
| 6.6 | $0-$5k | 2.18 |

## Summary

A vulnerability marked as critical has been reported in SourceCodester/jkev Record Management System 1.0. Affected by this issue is some unknown functionality of the file *index.php* of the component *Login*. This manipulation of the argument *Username* causes sql injection. This vulnerability is registered as CVE-2026-5575. Remote exploitation of the attack is possible. Furthermore, an exploit is available.

## Details

A vulnerability was found in SourceCodester/jkev Record Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown code of the file *index.php* of the component *Login*. The manipulation of the argument `UserName` with an unknown input leads to a sql injection vulnerability. The CWE definition for the vulnerability is 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. As an impact it is known to affect confidentiality, integrity, and availability.

The advisory is shared at github.com. This vulnerability is known as CVE-2026-5575. The exploitation appears to be easy. The attack can be launched remotely. The exploitation doesn't need any form of authentication. Technical details and also a public exploit are known. MITRE ATT&CK project uses the attack technique T1505 for this issue.

It is possible to download the exploit at github.com. It is declared as proof-of-concept. By approaching the search of inurl:index.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 entries are available at VDB-350703, VDB-350704, VDB-350710 and VDB-352365.

## Product

**Vendor**

- jkev
- SourceCodester

**Name**

- Record Management System

**Version**

- 1.0

**License**

- free

## 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

**Advisory**: github.com
**Status**: Not defined

**CVE**: CVE-2026-5575 (🔒)
**GCVE (CVE)**: GCVE-0-2026-5575
**GCVE (VulDB)**: GCVE-100-355345
**scip Labs**: https://www.scip.ch/en/?labs.20161013
**See also**: 🔒

## Entry

**Created**: 04/04/2026 04:50 PM
**Changes**: 04/04/2026 04:50 PM (56)
**Complete**: 🔍
**Submitter**: chenkh
**Cache ID**: 4:040:179

## Submit

**Accepted**

- Submit #783472: jkev Personnel Record Management System V1.0 SQL Injection (by chenkh)

## Discussion

No comments yet. Languages: en.

Please log in to comment.