



VDB-356270 · CVE-2026-5823 · GCVE-100-356270

# ITSOURCECODE CONSTRUCTION MANAGEMENT SYSTEM 1.0 BORROWED\_TOOL\_REPORT.PHP HOME SQL INJECTION

CVSS Meta Temp Score ?

5.7

Current Exploit Price (≈) ?

\$0-\$5k

CTI Interest Score ?

1.38

## Summary

A vulnerability described as **critical** has been identified in [itsourcecode Construction Management System 1.0](#). This affects an unknown part of the file `/borrowed_tool_report.php`. Such manipulation of the argument `Home` leads to sql injection. This vulnerability is referenced as [CVE-2026-5823](#). It is possible to launch the attack remotely. Furthermore, an exploit is available.

## Details

A vulnerability was found in [itsourcecode Construction Management System 1.0](#) and classified as **critical**. Affected by this issue is an unknown code block of the file `/borrowed_tool_report.php`. The manipulation of the argument `start` with an unknown input leads to a sql injection vulnerability. Using CWE to declare the problem leads to [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. Impacted is confidentiality, integrity, and availability.

The advisory is available at [github.com](#). This vulnerability is handled as [CVE-2026-5823](#). The exploitation is known to be easy. The attack may be launched remotely. Technical details as well as a public exploit are known. This vulnerability is assigned to **T1505** by the MITRE ATT&CK project.

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

### Vendor

- [itsourcecode](#)

### Name

- [Construction Management System](#)

### Version

- [1.0](#)

### License

- [free](#)

### Website

- Vendor: <https://itsourcecode.com/>

## CPE 2.3

- 

## CPE 2.2

- 

## CVSSv4

VulDB Vector: 

VulDB Reliability: 

## CVSSv3

VulDB Meta Base Score: 6.3

VulDB Meta Temp Score: 5.7

VulDB Base Score: 6.3

VulDB Temp Score: 5.7

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

04/08/2026		Advisory disclosed
04/08/2026	+0 days	VulDB entry created
04/08/2026	+0 days	VulDB entry last update

## Sources

**Vendor:** [itsourcecode.com](https://itsourcecode.com)

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

**Status:** Not defined

**CVE:** [CVE-2026-5823](#) (🗝️)

**GCVE (CVE):** [GCVE-0-2026-5823](#)

**GCVE (VulDB):** [GCVE-100-356270](#)

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

## Entry

**Created:** 04/08/2026 06:52 PM

**Changes:** 04/08/2026 06:52 PM (55)

**Complete:** 🔍

**Submitter:** [cm7ai](#)

**Cache ID:** 20:9CB:179

## Submit

**Accepted**

- [Submit #788299](#): itsourcecode Construction Management System V1.0 SQL Injection (by cm7ai)

## Discussion

No comments yet. Languages: en.

[Please log in to comment.](#)