



VDB-354388 · CVE-2026-5237 · GCVE-100-354388

ITSOURCECODE PAYROLL MANAGEMENT SYSTEM 1.0 PARAMETER /MANAGE_USER.PHP ID SQL INJECTION

CVSS Meta Temp Score

6.6

Current Exploit Price (≈)

\$0-\$5k

CTI Interest Score

2.31

Summary

A vulnerability was found in [itsourcecode Payroll Management System 1.0](#). It has been declared as **critical**. Affected by this issue is some unknown functionality of the file `/manage_user.php` of the component *Parameter Handler*. Executing a manipulation of the argument `ID` can lead to sql injection. This vulnerability appears as [CVE-2026-5237](#). The attack may be performed from remote. In addition, an exploit is available.

Details

A vulnerability has been found in [itsourcecode Payroll Management System 1.0](#) and classified as critical. This vulnerability affects some unknown processing of the file `/manage_user.php` of the component *Parameter Handler*. The manipulation of the argument `id` 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 for download at [github.com](#). This vulnerability was named [CVE-2026-5237](#). The exploitation appears to be easy. The attack can be initiated remotely. No form of authentication is required for a successful exploitation. Technical details and also a public exploit are known. The MITRE ATT&CK project declares the attack technique as [T1505](#).

It is possible to download the exploit at [github.com](#). It is declared as proof-of-concept. By approaching the search of `inurl:manage_user.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.

See [VDB-263894](#), [VDB-272582](#), [VDB-273156](#) and [VDB-273341](#) for similar entries.

Product

Vendor

- [itsourcecode](#)

Name

- [Payroll 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: 7.3

VulDB Meta Temp Score: 6.6

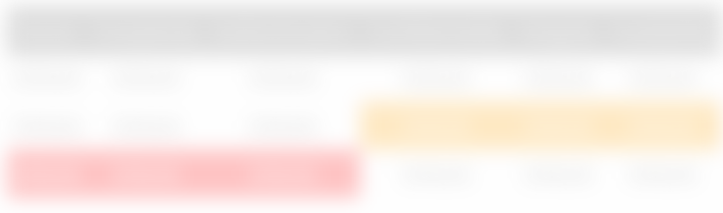
VulDB Base Score: 7.3

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

03/31/2026	█		Advisory disclosed
03/31/2026	█	+0 days	VulDB entry created
03/31/2026	█	+0 days	VulDB entry last update

Sources

Vendor: itsourcecode.com

Advisory: github.com

Status: Not defined

CVE: [CVE-2026-5237](#) (🗝️)

GCVE (CVE): [GCVE-0-2026-5237](#)

GCVE (VulDB): [GCVE-100-354388](#)

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

See also: 🗝️

Entry

Created: 03/31/2026 04:19 PM

Changes: 03/31/2026 04:19 PM (56)

Complete: 🔍

Submitter: [s1incere](#)

Cache ID: 52:674:179

Submit

Accepted

- [Submit #780474](#): itsourcecode Payroll Management System - V1.0 Argument Injection (by s1incere)

Discussion

No comments yet. Languages: en.

[Please log in to comment.](#)