VDB-307345 · CVE-2025-4248 · GCVE-100-307345

SOURCECODESTER SIMPLE TO-DO LIST SYSTEM 1.0 /COMPLETE_TASK.PHP ID SQL INJECTION

A vulnerability has been found in SourceCodester Simple To-Do List System 1.0 and classified as critical. Affected by this vulnerability is an unknown part of the file */complete_task.php*. 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 at github.com. This vulnerability is known as CVE-2025-4248. The exploitation appears to be easy. The attack can be launched remotely. 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:complete_task.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-307344.

Product

Vendor

- SourceCodester

Name

- Simple To-Do List System

Version

- 1.0

License

- free

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA CVSS-B Score: 🔒
CNA CVSS-BT Score: 🔒
CNA Vector: 🔒

CVSSv3

VulDB Meta Base Score: 6.3
VulDB Meta Temp Score: 6.0

VulDB Base Score: 6.3
VulDB Temp Score: 5.7
VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA Base Score: 6.3
CNA Vector: 🔒

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Sql injection
CWE: CWE-89 / CWE-74 / CWE-707
CAPEC: 🔒

ATT&CK: 🔒

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

05/03/2025		Advisory disclosed
05/03/2025	+0 days	VulDB entry created
05/04/2025	+1 days	VulDB entry last update

Sources

Vendor: sourcecodester.com

Advisory: github.com
Status: Not defined

CVE: CVE-2025-4248 (🔒)
GCVE (CVE): GCVE-0-2025-4248
GCVE (VulDB): GCVE-100-307345
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 05/03/2025 02:58 PM
Updated: 05/04/2025 10:38 AM
Changes: 05/03/2025 02:58 PM (55), 05/04/2025 10:38 AM (30)
Complete: 🔍
Submitter: zonesec
Cache ID: 5:210:101

Submit

Accepted

- Submit #562700: SourceCodester Simple To-Do List System 1.0 SQL Injection (by zonesec)

Discussion

No comments yet. Languages: en.

Please log in to comment.