



VDB-204575 · CVE-2022-2492

SOURCECODESTER LIBRARY MANAGEMENT SYSTEM 1.0 /INDEX.PHP ROLLNO SQL INJECTION

CVSS Meta Temp Score ?

6.9

Current Exploit Price (≈) ?

\$0-\$5k

CTI Interest Score ?

0.15

A vulnerability was found in SourceCodester Library Management System 1.0 (Library Management System Software) and classified as critical. This issue affects an unknown function of the file `/index.php`. The manipulation of the argument `RollNo` with the input value `admin' AND (SELECT 2625 FROM (SELECT(SLEEP(5)))MdIL) AND 'KXmq'='KXmq&Password=1231312312` leads to a sql injection vulnerability. Using CWE to declare the problem leads to CWE-89. The software 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 weakness was published 07/20/2022. It is possible to read the advisory at github.com. The identification of this vulnerability is CVE-2022-2492. Technical details as well as a public exploit are known. The attack technique deployed by this issue is T1505 according to MITRE ATT&CK.

It is declared as proof-of-concept. The exploit is available at github.com. By approaching the search of `inurl:index.php` it is possible to find vulnerable targets with Google Hacking. The code used by the exploit is:

```
POST /index.php HTTP/1.1
```

```
Host: www.l-ms.com
```

```
Cache-Control: no-cache
```

```
Content-Type: application/x-www-form-urlencoded
```

```
Content-Length: 111
```

```
RollNo=admin' AND (SELECT 2625 FROM (SELECT(SLEEP(5)))MdIL) AND 'KXmq'='KXmq&Password=1231312312&signin=Sign In
```

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

Product

Type

- Library Management System Software

Vendor

SourceCodester

- SourceCodester

Name

- Library Management System

License

- free

CPE 2.3

- 

CPE 2.2

- 

CVSSv3

VulDB Meta Base Score: 7.1

VulDB Meta Temp Score: 6.9

VulDB Base Score: 6.3

VulDB Temp Score: 5.7


VulDB Vector: 

VulDB Reliability: 

NVD Base Score: 8.8

NVD Vector: 

CNA Base Score: 6.3

CNA Vector (VulDB): 

CVSSv2



VulDB Base Score: 

VulDB Temp Score: 

VulDB Reliability: 

Exploiting

Class: Sql injection

CWE: CWE-89 / CWE-74 / CWE-707

ATT&CK: T1505

Local: No

Remote: Yes

Availability: 

Access: Public

Status: Proof-of-Concept

Download: 

Google Hack: 

EPSS Score: 

EPSS Percentile: 

Price Prediction: 

Current Price Estimation: 

Threat Intelligence

Interest: 

Active Actors: 

Active APT Groups: 

Countermeasures

Recommended: no mitigation known

Status: 

0-Day Time: 

Timeline

07/20/2022		Advisory disclosed
07/20/2022	+0 days	CVE reserved

07/20/2022	+0 days	CVE received
07/20/2022	+0 days	VulDB entry created
08/15/2022	+26 days	VulDB last update

Sources

Advisory: github.com

Status: Not defined

CVE: CVE-2022-2492 (🔒)

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

Entry

Created: 07/20/2022 11:17 AM

Updated: 08/15/2022 10:46 AM

Changes: 07/20/2022 11:17 AM (44), 08/15/2022 10:35 AM (2), 08/15/2022 10:41 AM (21), 08/15/2022 10:46 AM (1)

Complete: 🔍

Submitter: webray.com.cn

Discussion

No comments yet. Languages: en.

Please log in to comment.