SOURCECODESTER GUEST MANAGEMENT SYSTEM FRONT.PHP RID SQL INJECTION

CVSS Meta Temp Score ?	Current Exploit Price (≈) ?	CTI Interest Score ?
5.7	$0-$5k	0.00

A vulnerability, which was classified as critical, has been found in SourceCodester Guest Management System (unknown version). This issue affects an unknown part of the file */guestmanagement/front.php*. The manipulation of the argument `rid` with an unknown input 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 shared 08/16/2022. The advisory is shared at s1.ax1x.com. The identification of this vulnerability is CVE-2022-2847. Technical details as well as a public exploit are known. MITRE ATT&CK project uses the attack technique T1505 for this issue.

It is declared as proof-of-concept. The exploit is available at s1.ax1x.com. By approaching the search of inurl:guestmanagement/front.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

- SourceCodester

Name

- Guest Management System

CPE 2.3

- 🔒

CPE 2.2

- 🔒

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
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

08/16/2022		Advisory disclosed
08/16/2022	+0 days	CVE reserved
08/16/2022	+0 days	VulDB entry created
09/17/2022	+32 days	VulDB last update

Sources

Advisory: s1.ax1x.com
Status: Not defined

CVE: CVE-2022-2847 (🔒)
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 08/16/2022 04:01 PM
Updated: 09/17/2022 08:06 AM
Changes: 08/16/2022 04:01 PM (40), 09/17/2022 08:06 AM (2)
Complete: 🔍
Submitter: qidian

Discussion

No comments yet. Languages: en.

Please log in to comment.