VDB-207001 · CVE-2022-2957

SOURCECODESTER SIMPLE AND NICE SHOPPING CART SCRIPT /MKSHOP/MEN/PROFILE.PHP MEM_ID SQL INJECTION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
5.7	$0-$5k	0.10

A vulnerability classified as critical was found in SourceCodester Simple and Nice Shopping Cart Script (affected version unknown). Affected by this vulnerability is an unknown code of the file */mkshop/Men/profile.php*. The manipulation of the argument `mem_id` with an unknown input leads to a sql injection vulnerability. The CWE definition for the vulnerability is 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. As an impact it is known to affect confidentiality, integrity, and availability.

The weakness was released 08/23/2022. The advisory is shared at s1.ax1x.com. This vulnerability is known as CVE-2022-2957. Technical details and also a public exploit are known. MITRE ATT&CK project uses the attack technique T1505 for this issue.

It is declared as proof-of-concept. It is possible to download the exploit at s1.ax1x.com. By approaching the search of inurl:mkshop/Men/profile.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

- Simple and Nice Shopping Cart Script

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

08/23/2022		Advisory disclosed
08/23/2022	+0 days	CVE reserved
08/23/2022	+0 days	VulDB entry created
09/24/2022	+32 days	VulDB last update

Sources

Advisory: s1.ax1x.com
Status: Not defined

CVE: CVE-2022-2957 (🔒)
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 08/23/2022 10:43 AM
Updated: 09/24/2022 03:32 PM
Changes: 08/23/2022 10:43 AM (40), 09/24/2022 03:32 PM (2)
Complete: 🔍
Submitter: qidian

Discussion

No comments yet. Languages: en.

Please log in to comment.