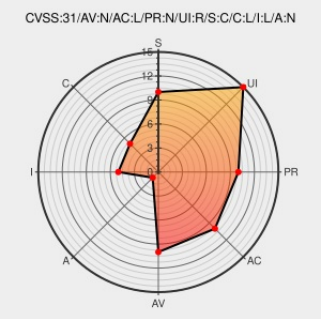
CVE-2023-3005

Published on: Not Yet Published

Last Modified on: 10/23/2023 08:07:29 AM UTC

CVE-2023-3005

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Local Service Search Engine Management System from Local Service Search Engine Management System Project contain the following vulnerability:

A vulnerability, which was classified as problematic, was found in SourceCodester Local Service Search Engine Management System 1.0. This affects an unknown part of the file /admin/ajax.php?action=save_area of the component POST Parameter Handler. The manipulation of the argument area with the input <script>alert(document.cookie)</script> leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-230349 was assigned to this vulnerability.

CVE-2023-3005 has been assigned by cna@vuldb.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **SourceCodester** - **Local Service Search Engine Management System** version **= 1.0**

CVSS3 Score: 6.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVE References

Description	Tags	Link
CVE-2023-3005: SourceCodester Local Service Search Engine Management System POST Parameter cross site scripting	vuldb.com text/html	MISC vuldb.com/?id.230349
Login required	vuldb.com text/html Inactive Link Not Archived	MISC vuldb.com/?ctiid.230349

CVE/XSS.md at main · sikii7/CVE · GitHub

github.com
text/html

MISC
github.com/sikii7/CVE/blob/main/XSS.md

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Local Service Search Engine Management System Project	Local Service Search Engine Management System	1.0	All	All	All

cpe:2.3:a:local_service_search_engine_management_system_project:local_service_search_engine_management_system:1.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→