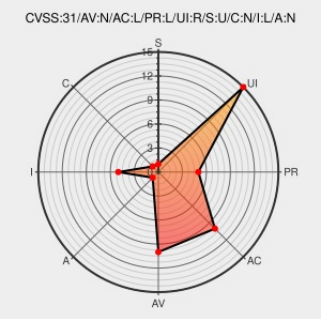
CVE-2022-4561

Published on: Not Yet Published

Last Modified on: 12/21/2022 06:35:00 PM UTC

CVE-2022-4561

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



Certain versions of Semantic Drilldown from Mediawiki contain the following vulnerability:

A vulnerability classified as problematic has been found in SemanticDrilldown Extension. Affected is the function printFilterLine of the file includes/specials/SDBrowseDataPage.php of the component GET Parameter Handler. The manipulation of the argument value leads to cross site scripting. It is possible to launch the attack remotely. The name of the patch is 6e18cf740a4548166c1d95f6d3a28541d298a3aa. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-215964.

CVE-2022-4561 has been assigned by cna@vuldb.com to track the vulnerability - currently rated as MEDIUM severity.

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-2022-4561 | SemanticDrilldown Extension GET Parameter SDBrowseDataPage.php printFilterLine cross site scripting	vuldb.com text/html	MISC vuldb.com/?id.215964
Added anti XSS fix in SDBrowseDataPage.php · wikimedia/mediawiki-extensions-SemanticDrilldown@6e18cf7 · GitHub	github.com text/html	MISC github.com/wikimedia/mediawiki-extensions-SemanticDrilldown/commit/6e18cf740a4548166c1d95f6d3a28541d298a3aa

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	Mediawiki	Semantic Drilldown	All	All	All	All

cpe:2.3:a:mediawiki:semantic_drilldown:*:*:*:*:*:mediawiki:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/netcve	CVE-2022-4561	2022-12-16 19:45:48

← Previous ID

Next ID→