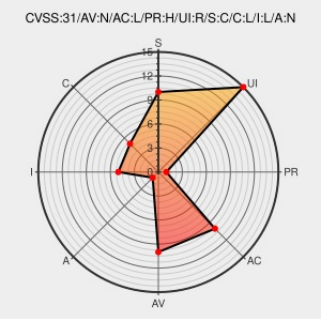
CVE-2022-3832

Published on: Not Yet Published

Last Modified on: 12/22/2022 10:00:00 PM UTC

CVE-2022-3832

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



Certain versions of External Media from External Media Project contain the following vulnerability:

The External Media WordPress plugin before 1.0.36 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).

CVE-2022-3832 has been assigned by contact@wpscan.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Unknown** - **External Media** version **= 0**

CVSS3 Score: 4.8 - MEDIUM

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

CVE References

Description	Tags	Link
Just a moment...	wpscan.com text/html Inactive Link Not Archived	MISC wpscan.com/vulnerability/458ec2fd-4175-4cb4-b334-b63f6e643b92

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	External Media Project	External Media	All	All	All	All

cpe:2.3:a:external_media_project:external_media:*:*:*:*:*:wordpress:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-3832 : The External Media WordPress plugin before 1.0.36 does not sanitise and escape some of its settings… twitter.com/i/web/status/1…	2022-12-19 14:04:09
/r/netcve	CVE-2022-3832	2022-12-19 14:40:34

← Previous ID

Next ID→