CVE-2023-4836

Published on: Not Yet Published

Last Modified on: 10/31/2023 02:23:00 PM UTC

CVE-2023-4836

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

Certain versions of WordPress File Sharing Plugin from Unknown contain the following vulnerability:

The WordPress File Sharing Plugin WordPress plugin before 2.0.5 does not check authorization before displaying files and folders, allowing users to gain access to those filed by manipulating IDs which can easily be brute forced

CVE-2023-4836 has been assigned by contact@wpscan.com to track the vulnerability

Affected Vendor/Software: **Unknown** - **WordPress File Sharing Plugin** version **< 2.0.5**

CVE References

Description	Tags	Link
CVE-2023-4836 - User Private Files - IDOR to Sensitive data and private files exposure / leak of info - POC - Use only certified WordPress plugins for your website	research.cleantalk.org text/html	MISC research.cleantalk.org/cve-2023-4836-user-private-files-idor-to-sensitive-data-and-private-files-exposure-leak-of-info-poc
Just a moment...	wpscan.com text/html Inactive Link Not Archived	MISC wpscan.com/vulnerability/c17f2534-d791-4fe3-b45b-875777585dc6

There are currently no QIDs associated with this CVE

Known Affected Software

Vendor	Product	Version
Unknown	WordPress_File_Sharing_Plugin	< 2.0.5

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→