CVE-2023-5241

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2023-5241
State	PUBLIC
Assigner	security@wordfence.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-19 06:15:00 UTC
Updated	2023-11-07 04:23:00 UTC
Description	The AI ChatBot for WordPress is vulnerable to Directory Traversal in versions up to, and including, 4.8.9 as well as 4.9.2 via

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Quantumcloud	Ai Chatbot	All	All	All	All
Application	Quantumcloud	Ai Chatbot	4.9.2	All	All	All

References

Reference	Sour
403 Forbidden	MISC
AI ChatBot <= 4.8.9 - Authenticated (Subscriber+) Directory Traversal to Arbitrary File Write via qcld_openai_upload_pagetraining_file	MISC
403 Forbidden	MISC
WordPress AI ChatBot 4.8.9 SQL Injection / Traversal / File Deletion ≈ Packet Storm	MISC
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.