



CVE-2023-23883

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2023-23883
State	PUBLIC
Assigner	audit@patchstack.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-09 11:15:00 UTC
Updated	2023-05-12 09:26:00 UTC
Description	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in David Gwyer WP Content Filter plugin <= 3.0.1 versions.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product
Application	Wp Content Filter - Censor All Offensive Content From Your Site Project	Wp Content Filter - Censor All Offensive Content Fro

References

Reference

- WordPress WP Content Filter – Censor All Offensive Content From Your Site plugin <= 3.0.1 - Cross Site Scripting (XSS) vulnerability - Patch
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report