



CVE-2023-1159

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-1159
State	PUBLIC
Assigner	security@wordfence.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-02 07:15:00 UTC
Updated	2023-11-07 04:02:00 UTC
Description	The Bookly plugin for WordPress is vulnerable to Stored Cross-Site Scripting via service titles in versions up to, and includi

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Booking-wp-plugin	Bookly	All	All	All	All

References

Reference	Source	Link	Tags
Bookly <= 21.7 - Authenticated (Admin+) Stored Cross-Site Scripting	MISC	www.wordfence.com	
403 Forbidden	MISC	plugins.trac.wordpress.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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