



CVE-2023-29093

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

Summary

CVE	CVE-2023-29093
State	PUBLIC
Assigner	audit@patchstack.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-26 06:15:00 UTC
Updated	2023-07-03 19:19:00 UTC
Description	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PI Websolution Condi

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Lang
Application	Piwebsolution	Conditional Cart Fee / Extra Charge Rule For Woocommerce Extra Fees	All	All	All	All

References

Reference	Source	Link
WordPress Conditional extra fees for woocommerce plugin <= 1.0.96 - Cross Site Scripting (XSS) vulnerability - Patchstack	MISC	pa
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nv

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