



CVE-2023-37988

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

Summary

CVE	CVE-2023-37988
State	PUBLIC
Assigner	audit@patchstack.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-10 11:15:00 UTC
Updated	2023-10-19 20:27:00 UTC
Description	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Creative Solutions Contact Form Generator plugin <= 2.5.5 ve

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Creative-solutions	Contact Form Generator	All	All	All	All

References

Reference	Source	Link
WordPress Contact Form Generator 2.5.5 Cross Site Scripting ≈ Packet Storm	MISC	packetsto
WordPress Contact Form Generator plugin <= 2.5.5 - Reflected Cross Site Scripting (XSS) vulnerability - Patchstack	MISC	patchstac
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

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