



CVE-2022-38075

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

Summary

CVE	CVE-2022-38075
State	PUBLIC
Assigner	audit@patchstack.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-18 19:15:00 UTC
Updated	2022-11-21 01:46:00 UTC
Description	Cross-Site Request Forgery (CSRF) vulnerability leading to Stored Cross-Site Scripting (XSS) in Mantenimiento web plugin

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Webartesanal	Mantenimiento Web	All	All	All	All

References

Reference

- WordPress Mantenimiento web plugin <= 0.13 - Cross-Site Request Forgery (CSRF) vulnerability leading to Stored Cross-Site Scripting (XSS)
- CVE Program record
- NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

LEGACY: Vulnerability discovered by Rasi Afeef (Patchstack Alliance)

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

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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