



CVE-2021-36833

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

Summary

CVE	CVE-2021-36833
State	PUBLIC
Assigner	audit@patchstack.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-20 20:15:00 UTC
Updated	2022-10-19 18:54:00 UTC
Description	Authenticated (admin or higher user role) Stored Cross-Site Scripting (XSS) vulnerability in ibericode's MC4WP plugin <= 4

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mailchimp For Wordpress Project	Mailchimp For Wordpress	All	All	All	All
Application	Mc4wp	Mc4wp	All	All	All	All

References

Reference	Source	Link
WordPress MC4WP plugin <= 4.8.6 - Authenticated Stored Cross-Site Scripting (XSS) vulnerability - Patchstack	CONFIRM	patchstack.com
MC4WP: Mailchimp for WordPress – WordPress plugin WordPress.org	CONFIRM	wordpress.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Vulnerability discovered by Asif Nawaz Minhas (Patchstack Alliance)

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#)