



CVE-2021-23150

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

Summary

CVE	CVE-2021-23150
State	PUBLIC
Assigner	audit@patchstack.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-18 18:15:00 UTC
Updated	2023-11-07 03:30:00 UTC
Description	Authenticated (admin+) Stored Cross-Site Scripting (XSS) vulnerability discovered in AMP for WP – Accelerated Mobile Pa

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ampforwp	Accelerated Mobile Pages	All	All	All	All

References

Reference

- AMP for WP – Accelerated Mobile Pages – WordPress plugin | WordPress.org
- WordPress AMP for WP – Accelerated Mobile Pages plugin <= 1.0.77.31 - Authenticated Stored Cross-Site Scripting (XSS) vulnerability - Pat
- WordPress AMP for WP – Accelerated Mobile Pages plugin <= 1.0.77.31 - Authenticated Stored Cross-Site Scripting (XSS) vulnerability - Pat
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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