



CVE-2020-36745

Published on: Not Yet Published

Last Modified on: 07/07/2023 03:40:00 AM UTC

CVE-2020-36745

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Wp Project Manager](#) from [Wedevs](#) contain the following vulnerability:

The WP Project Manager plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.4.0. This is due to missing or incorrect nonce validation on the `do_updates()` function. This makes it possible for unauthenticated attackers to trigger updates via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.

CVE-2020-36745 has been assigned by security@wordfence.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **wedevs - WP Project Manager – Task, team, and project management plugin featuring kanban board and gantt charts** version < 2.4.1

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
25 WordPress plugins vulnerable to CSRF attacks. – NinTechNet	blog.nintech.net.com text/html	MISC blog.nintech.net.com/25-wordpress-plugins-vulnerable-to-csrf-attacks/
More WordPress plugins and themes vulnerable to CSRF attacks. – NinTechNet	blog.nintech.net.com text/html	MISC blog.nintech.net.com/more-wordpress-plugins-and-themes-vulnerable-to-csrf-attacks/
403 Forbidden	plugins.trac.wordpress.org text/html Inactive Link Not Archived	MISC plugins.trac.wordpress.org/browser/wedevs-project-manager/tags/2.4.1/core/Upgrades/Upgrade.php?rev=2368374#L179

Multiple WordPress plugins fixed CSRF vulnerabilities (part 3). – NinTechNet	blog.nintech.net.com text/html	MISC blog.nintech.net.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-3/
Multiple WordPress plugins fixed CSRF vulnerabilities (part 2). – NinTechNet	blog.nintech.net.com text/html	MISC blog.nintech.net.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-2/
WP Project Manager <= 2.4.0 - Cross-Site Request Forgery Bypass	www.wordfence.com text/html	MISC www.wordfence.com/threat-intel/vulnerabilities/id/456c13f5-4a8b-4eea-a2a0-f37f8508551b?source=cve
Multiple WordPress plugins fixed CSRF vulnerabilities (part 4). – NinTechNet	blog.nintech.net.com text/html	MISC blog.nintech.net.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-4/
Multiple WordPress plugins fixed CSRF vulnerabilities (part 5). – NinTechNet	blog.nintech.net.com text/html	MISC blog.nintech.net.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-5/
Multiple WordPress plugins fixed CSRF vulnerabilities (part 1). – NinTechNet	blog.nintech.net.com text/html	MISC blog.nintech.net.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-1/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wdevs	Wp Project Manager	All	All	All	All
cpe:2.3:a:wdevs:wp_project_manager:*:*:*:*:wordpress:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)