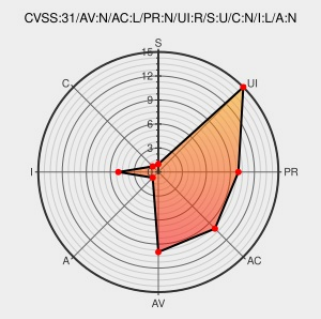
CVE-2021-4416

Published on: Not Yet Published

Last Modified on: 11/07/2023 03:40:00 AM UTC

CVE-2021-4416

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Wp-mpdf from Wp-mpdf Project contain the following vulnerability:

The wp-mpdf plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.5.1. This is due to missing or incorrect nonce validation on the mpdf_admin_savepost() function. This makes it possible for unauthenticated attackers to save post data via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.

CVE-2021-4416 has been assigned by security@wordfence.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **fkrauthan** - **wp-mpdf** version **<= 3.5.1**

CVSS3 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
25 WordPress plugins vulnerable to CSRF attacks. – NinTechNet	blog.nintechnet.com text/html	MISC blog.nintechnet.com/25-wordpress-plugins-vulnerable-to-csrf-attacks/
More WordPress plugins and themes vulnerable to CSRF attacks. – NinTechNet	blog.nintechnet.com text/html	MISC blog.nintechnet.com/more-wordpress-plugins-and-themes-vulnerable-to-csrf-attacks/
Multiple WordPress plugins fixed CSRF vulnerabilities (part 3). – NinTechNet	blog.nintechnet.com text/html	MISC blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-3/
Multiple WordPress plugins fixed CSRF vulnerabilities (part 2). – NinTechNet	blog.nintechnet.com text/html	MISC blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-2/

wp-mpdf <= 3.5.1 - Cross-Site Request Forgery Bypass	www.wordfence.com text/html	MISC www.wordfence.com/threat-intel/vulnerabilities/id/c47386ee-25c8-4a77-92e8-5a82afc9c826?source=cve
Multiple WordPress plugins fixed CSRF vulnerabilities (part 4). – NinTechNet	blog.nintechnet.com text/html	MISC blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-4/
Multiple WordPress plugins fixed CSRF vulnerabilities (part 5). – NinTechNet	blog.nintechnet.com text/html	MISC blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-5/
403 Forbidden	plugins.trac.wordpress.org text/html Inactive Link Not Archived	MISC plugins.trac.wordpress.org/changeset/2549363/wp-mpdf/trunk/wp-mpdf.php
Multiple WordPress plugins fixed CSRF vulnerabilities (part 1). – NinTechNet	blog.nintechnet.com text/html	MISC blog.nintechnet.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-1/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wp-mpdf Project	Wp-mpdf	All	All	All	All

cpe:2.3:a:wp-mpdf_project:wp-mpdf:*:*:*:*:*:wordpress:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-4416 : The wp-mpdf plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and… twitter.com/i/web/status/1…	2023-07-12 04:09:40
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2021-4416 The wp-mpdf plugin for WordPress is vulnerable to Cross-Site Reque… twitter.com/i/web/status/1…	2023-07-12 05:11:02
@JohnJasonFallow	New vulnerability on the NVD: CVE-2021-4416 ift.tt/NB7O1mV	2023-07-12 05:12:45

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report