



# CVE-2021-4416

Published on: Not Yet Published

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

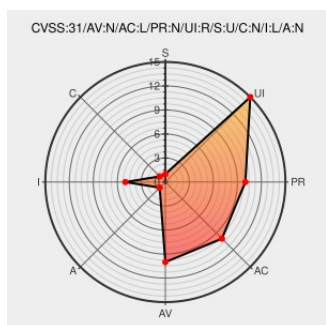
## CVE-2021-4416

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    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>LOW</b>          | <b>NONE</b>         |

## CVE References

| Description                                                                  | Tags                                                              | Link                                                                                               |
|------------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| 25 WordPress plugins vulnerable to CSRF attacks. – NinTechNet                | <a href="#">blog.nintech.net.com</a><br><a href="#">text/html</a> | <a href="#">blog.nintech.net.com/25-wordpress-plugins-vulnerable-to-csrf-attacks/</a>              |
| More WordPress plugins and themes vulnerable to CSRF attacks. – NinTechNet   | <a href="#">blog.nintech.net.com</a><br><a href="#">text/html</a> | <a href="#">blog.nintech.net.com/more-wordpress-plugins-and-themes-vulnerable-to-csrf-attacks/</a> |
| Multiple WordPress plugins fixed CSRF vulnerabilities (part 3). – NinTechNet | <a href="#">blog.nintech.net.com</a><br><a href="#">text/html</a> | <a href="#">blog.nintech.net.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-3/</a> |
| Multiple WordPress plugins fixed CSRF vulnerabilities (part 2). – NinTechNet | <a href="#">blog.nintech.net.com</a><br><a href="#">text/html</a> | <a href="#">blog.nintech.net.com/multiple-wordpress-plugins-fixed-csrf-vulnerabilities-part-2/</a> |

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

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](mailto: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                                              | <a href="#">Wp-mpdf Project</a> | <a href="#">Wp-mpdf</a> | 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... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 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... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2023-07-12 05:11:02 |
| @JohnJasonFallow | New vulnerability on the NVD: CVE-2021-4416 <a href="https://ift.tt/NB7O1mV">ift.tt/NB7O1mV</a>                                                                                                          | 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](https://status.cve.report)