



# CVE-2021-24388

Published on: 07/06/2021 12:00:00 AM UTC

Last Modified on: 02/15/2023 02:31:00 AM UTC

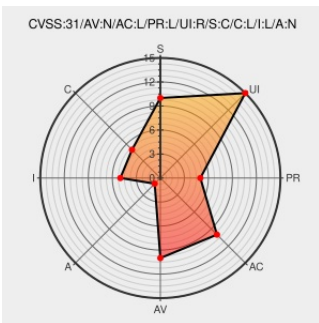
## CVE-2021-24388

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Vikrentcar Car Rental Management System](#) from [E4j](#) contain the following vulnerability:

In the VikRentCar Car Rental Management System WordPress plugin before 1.1.7, there is a custom filed option by which we can manage all the fields that the users will have to fill in before saving the order. However, the field name is not sanitised or escaped before being output back in the page, leading to a stored Cross-Site Scripting issue.

There is also no CSRF check done before saving the setting, allowing attackers to make a logged in admin set arbitrary Custom Fields, including one with XSS payload in it.

CVE-2021-24388 has been assigned by [contact@wpscan.com](mailto:contact@wpscan.com) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **E4J s.r.l. - VikRentCar Car Rental Management System** version < 1.1.7


CVSS3 Score: **5.4 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
<b>NETWORK</b>	<b>LOW</b>	<b>LOW</b>	<b>REQUIRED</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>CHANGED</b>	<b>LOW</b>	<b>LOW</b>	<b>NONE</b>

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
<b>NETWORK</b>	<b>MEDIUM</b>	<b>SINGLE</b>
Confidentiality Impact	Integrity Impact	Availability Impact
<b>NONE</b>	<b>PARTIAL</b>	<b>NONE</b>

## CVE References

Description	Tags	Link
Attention Required!   Cloudflare	<a href="#">wpscan.com</a> <a href="#">text/html</a> <span>Inactive Link</span> <span>Not Archived</span>	 CONFIRM <a href="https://wpscan.com/vulnerability/e3f6576f-08cb-4278-8c79-3ef4d0b85cd9">wpscan.com/vulnerability/e3f6576f-08cb-4278-8c79-3ef4d0b85cd9</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

### Exploit/POC from Github

In the VikRentCar Car Rental Management System WordPress plugin before 1.1.7, there is a custom filed option by which...

### Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	E4j	Vikrentcar Car Rental Management System	All	All	All	All

cpe:2.3:a:e4j:vikrentcar\_car\_rental\_management\_system:\*:\*:\*:\*:wordpress:\*:\*

### Discovery Credit

Satyender Yadav

### Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2024   |

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](https://status.cve.report)