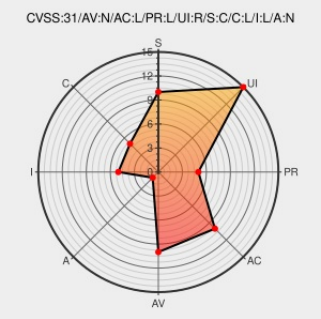
CVE-2021-37392

Published on: 07/26/2021 12:00:00 AM UTC

Last Modified on: 08/06/2021 04:21:00 PM UTC

CVE-2021-37392

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



Certain versions of Rpcms from Rpcms contain the following vulnerability:

In RPCMS v1.8 and below, the "nickname" variable is not properly sanitized before being displayed on page. When the API functions are enabled, the attacker can use API to update user nickname with XSS payload and achieve stored XSS. Users who view the articles published by the injected user will trigger the XSS.

CVE-2021-37392 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.4 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
RPCMS CVE Submission · GitHub	gist.github.com text/html	MISC gist.github.com/victomteng1997/bfa1e0e07dd22f7e0b13256eda79626f
GitHub - ralap-z/rpcms: RPCMS内容管理系	github.com	MISC github.com/ralap-z/RPCMS/

统 text/html

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	Rpcms	Rpcms	All	All	All	All

cpe:2.3:a:rpcms:rpcms:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-37392 : In RPCMS v1.8 and below, the "nickname" variable is not properly sanitized before being displayed… twitter.com/i/web/status/1…	2021-07-26 17:44:43

← 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 registred 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