CVE-2021-37394

Published on: 07/26/2021 12:00:00 AM UTC
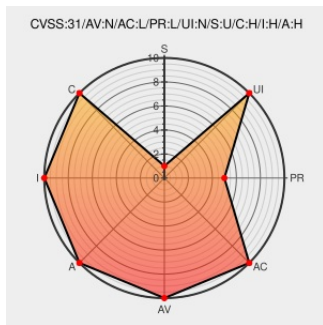
Last Modified on: 08/06/2021 04:11:00 PM UTC

CVE-2021-37394

[Source: Mitre] [Source: Nist] [Print: PDF 📄]

Certain versions of Rpcms from Rpcms contain the following vulnerability:

In RPCMS v1.8 and below, attackers can interact with API and change variable "role" to "admin" to achieve admin user registration.

CVE-2021-37394 has been assigned by Ⓜ cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE

Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

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内容管理系统	github.com text/html	⌗ MISC github.com/ralap-z/RPCMS/

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-2021-37394 : In RPCMS v1.8 and below, attackers can interact with API and change variable "role" to "admin" to… twitter.com/i/web/status/1…	2021-07-26 17:45:27

← Previous ID   Next ID→