CVE-2021-39210

Published on: 09/15/2021 12:00:00 AM UTC
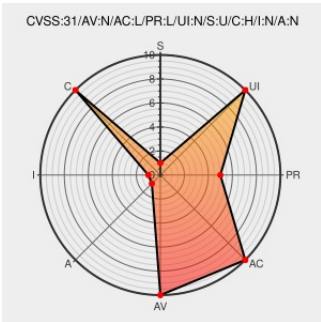
Last Modified on: 09/28/2021 04:40:00 PM UTC

CVE-2021-39210 - advisory for GHSA-hwxq-4c5f-m4v2

Source: Mitre	Source: Nist	Print: PDF 📄

Certain versions of Glpi from Glpi-project contain the following vulnerability:

GLPI is a free Asset and IT management software package. In versions prior to 9.5.6, the cookie used to store the autologin cookie (when a user uses the "remember me" feature) is accessible by scripts. A malicious plugin that could steal this cookie would be able to use it to autologin. This issue is fixed in version 9.5.6. As a workaround, one may avoid using the "remember me" feature.

CVE-2021-39210 has been assigned by ⚫ security-advisories@github.com to track the vulnerability - currently rated as `MEDIUM` severity.

Affected Vendor/Software: ⚫ **glpi-project** - **glpi** version **< 9.5.6**

CVSS3 Score: `6.5 - MEDIUM`

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

Scope	Confidentiality Impact	Integrity Impact	Availability Impact
`UNCHANGED`	`HIGH`	`NONE`	`NONE`

CVSS2 Score: `3.5 - LOW`

Access Vector	Access Complexity	Authentication
`NETWORK`	`MEDIUM`	`SINGLE`

Confidentiality Impact	Integrity Impact	Availability Impact
`PARTIAL`	`NONE`	`NONE`

CVE References

Description	Tags	Link

Description	Tags	Link
Release 9.5.6 · glpi-project/glpi · GitHub	`github.com` `text/html`	◯ MISC github.com/glpi-project/glpi/releases/tag/9.5.6
Autologin cookie accessible by scripts · Advisory · glpi-project/glpi · GitHub	`github.com` `text/html`	◯ CONFIRM github.com/glpi-project/glpi/security/advisories/GHSA-hwxq-4c5f-m4v2
huntr: Sensitive Cookie Without 'HttpOnly' Flag PHP Vulnerability in glpi	`huntr.dev` `text/html`	🔒 MISC huntr.dev/bounties/b2e99a41-b904-419f-a274-ae383e4925f2/

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	Glpi-project	Glpi	All	All	All	All

cpe:2.3:a:glpi-project:glpi:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
🐦 @CVEreport	CVE-2021-39210 : GLPI is a free Asset and IT management software package. In versions prior to 9.5.6, the cookie us… twitter.com/i/web/status/1…	2021-09-15 16:45:26

← Previous ID   Next ID→