

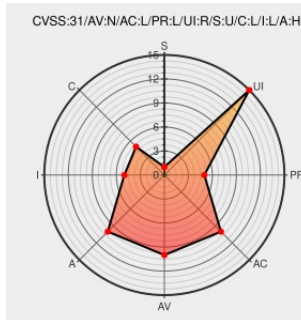


CVE-2022-31187

Published on: Not Yet Published

Last Modified on: 09/19/2022 02:08:00 PM UTC

CVE-2022-31187 - advisory for GHSA-43j5-xhvj-9236

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Glpi](#) from [Glpi-project](#) contain the following vulnerability:

GLPI stands for Gestionnaire Libre de Parc Informatique and is a Free Asset and IT Management Software package, that provides ITIL Service Desk features, licenses tracking and software auditing. Affected versions were found to not properly neutralize HTML tags in the global search context. Users are advised to upgrade to version 10.0.3 to resolve this issue. Users unable to upgrade should disable global search.

CVE-2022-31187 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [glpi-project](#) - [glpi](#) version $\geq 10.0.0$, $< 10.0.3$

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

CVE References

Description	Tags	Link
Fix handling of global search output · glpi-project/glpi@e248ed5 · GitHub	github.com text/html	MISC github.com/glpi-project/glpi/commit/e248ed5649d267c0f61a17d99b7bd6be4074aadb
Stored XSS through global search · Advisory · glpi-project/glpi · GitHub	github.com text/html	CONFIRM github.com/glpi-project/glpi/security/advisories/GHSA-43j5-xhvj-9236

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-2022-31187 : GLPI stands for Gestionnaire Libre de Parc Informatique and is a Free Asset and IT Management Soft... twitter.com/i/web/status/1...	2022-09-14 18:12:22
 /r/netcve	CVE-2022-31187	2022-09-14 19:38:59

[← 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 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](#)