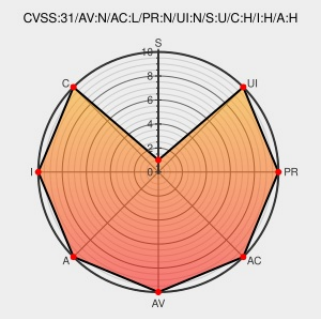
CVE-2022-31061

Published on: Not Yet Published

Last Modified on: 07/07/2022 04:47:00 PM UTC

CVE-2022-31061 - advisory for GHSA-w2gc-v2gm-q7wq

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



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

GLPI is a Free Asset and IT Management Software package, Data center management, ITIL Service Desk, licenses tracking and software auditing. In affected versions there is a SQL injection vulnerability which is possible on login page. No user credentials are required to exploit this vulnerability. Users are advised to upgrade as soon as possible. There are no known workarounds for this issue.

CVE-2022-31061 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **glpi-project** - **glpi** version **>= 9.3.0, < 9.5.8**

Affected Vendor/Software: **glpi-project** - **glpi** version **>= 10.0.0, < 10.0.2**

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
SQL injection on login page · Advisory · glpi-project/glpi · GitHub	github.com text/html	CONFIRM github.com/glpi-project/glpi/security/advisories/GHSA-w2gc-v2gm-q7wq
Merge pull request from GHSA-w2gc-v2gm-q7wq · glpi-project/glpi@21ae07d · GitHub	github.com text/html	MISC github.com/glpi-project/glpi/commit/21ae07d00d0b3230f6235386e98388cfc5bb0514

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

Exploit/POC from Github

PoC for GLPI CVE-2022-31061

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-2022-31061 : GLPI is a Free Asset and IT Management Software package, Data center management, ITIL Service Desk… twitter.com/i/web/status/1…	2022-06-28 18:07:12
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-31061 GLPI is a Free Asset and IT Management Software package, Data cen… twitter.com/i/web/status/1…	2022-06-28 19:55:55
@0_exploit	CVE-2022-31061 dlvr.it/ST15qn	2022-06-28 20:29:36
@LinInfoSec	Glpi - CVE-2022-31061: github.com/glpi-project/g…	2022-06-28 21:00:43
/r/netcve	CVE-2022-31061	2022-06-28 18:38:34

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report