



CVE-2019-1010310

Published on: 07/12/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:56 PM UTC

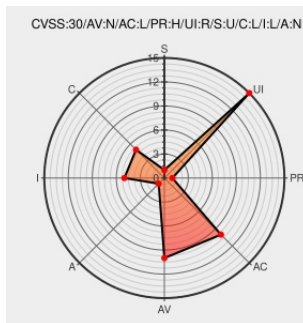
CVE-2019-1010310

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

GLPI GLPI Product 9.3.1 is affected by: Frame and Form tags Injection allowing admins to phish users by putting code in reminder description. The impact is: Admins can phish any user or group of users for credentials / credit cards. The component is: Tools > Reminder > Description .. Set the description to any iframe/form tags and apply.

The attack vector is: The attacker puts a login form, the user fills it and clicks on submit .. the request is sent to the attacker domain saving the data. The fixed version is: 9.4.1.

CVE-2019-1010310 has been assigned by [GSD](#) [cve-assign@distributedweaknessfiling.org](#) to track the vulnerability - currently rated as **LOW** severity.

Affected Vendor/Software: [GSD](#) **GLPI - GLPI Product** version **9.3.1 [fixed: 9.4.1]**

CVSS3 Score: **3.5 - LOW**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	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				
Prevent form and iframe in tinymce contents by trasher · Pull Request #5519 · glpi-project/glpi · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/glpi-project/glpi/pull/5519				
Release 9.3.1 · glpi-project/glpi · GitHub	Release Notes Third Party Advisory github.com text/html	MISC github.com/glpi-project/glpi/releases/tag/9.3.1				
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	9.3.1	All	All	All
Application	Glpi-project	Glpi	9.3.1	All	All	All
cpe:2.3:a:glpi-project:glpi:9.3.1:*:*:*:*:*:						
cpe:2.3:a:glpi-project:glpi:9.3.1:*:*:*:*:*:						
No vendor comments have been submitted for this CVE						
← Previous ID Next ID →						