

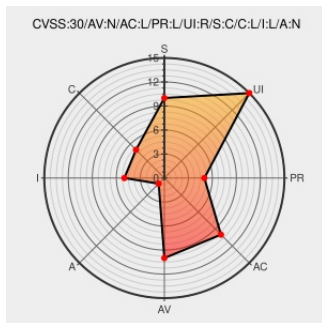


CVE-2019-1010307

Published on: 07/15/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:57 PM UTC

CVE-2019-1010307

[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: Cross Site Scripting (XSS). The impact is: All dropdown values are vulnerable to XSS leading to privilege escalation and executing js on admin. The component is: /glpi/ajax/getDropDownValue.php. The attack vector is: 1- User Create a ticket , 2- Admin opens another ticket and click on the "Link Tickets" feature, 3- a request to the endpoint fetches js and executes it.

CVE-2019-1010307 has been assigned by [GSD](#) [cve-assign@distributedweaknessfiling.org](#) to track the vulnerability - currently rated as **MEDIUM** severity.

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

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

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
-------------	------	------

Description

Tags

Link

glpi/getDropdownValue.php at 9.4/bugfixes · glpi-project/glpi · GitHub

Exploit

Third Party Advisory

github.com

text/html

MISC

github.com/glpi-project/glpi/blob/9.4/bugfixes/ajax/getDropdownValue.php

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 →