



CVE-2019-13239

Published on: 07/04/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:46 PM UTC

CVE-2019-13239

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

inc/user.class.php in GLPI before 9.4.3 allows XSS via a user picture.

CVE-2019-13239 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
	Exploit Third Party Advisory www.synacktiv.com application/pdf	MISC www.synacktiv.com/ressources/advisories/GLPI_9.4.0_stored_XSS.pdf

 MISC github.com/glpj-project/glpj/commit/c2aa7a7cd6af28be3809acc7e7842d2d2008c0fb

 github.com/glipi-project/glipi/releases/tag/9.4.3

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Application	Glpi-project	Glpi	All	All	All	All
Application	Glpi-project	Glpi	All	All	All	All
cpe:2.3:a:glpi-project:glpi:*.*.*.*.*.*.*.*.						
cpe:2.3:a:glpi-project:glpi:*.*.*.*.*.*.*.*.						

Next ID→