

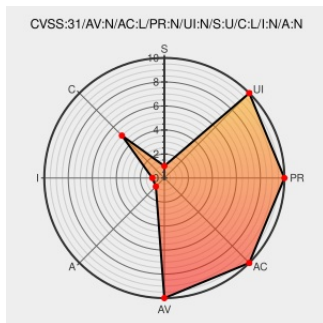


CVE-2020-15217

Published on: 10/07/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:41 PM UTC

CVE-2020-15217 - advisory for GHSA-x9hg-j29f-wvvv

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

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

In GLPI before version 9.5.2, there is a leakage of user information through the public FAQ. The issue was introduced in version 9.5.0 and patched in 9.5.2. As a workaround, disable public access to the FAQ.

CVE-2020-15217 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **glpi-project** - **glpi** version **>= 9.5.0, < 9.5.2**

CVSS3 Score: **5.3 - MEDIUM**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
Merge pull request from GHSA-x9hg-j29f-wvvv - alni-project/alni@39e2559 · GitHub	Patch Third Party Advisory	CONFIRM github.com/alni-project/alni/commit/39e25591efddc560e3679ab07e443ee6198705e2

[illegible]

text/html