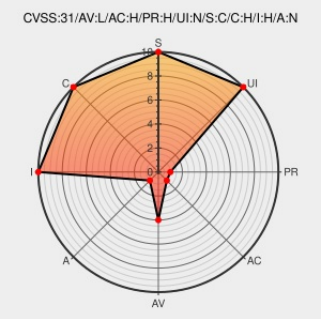
CVE-2020-5248

Published on: 05/12/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:03 PM UTC

CVE-2020-5248 - advisory for GHSA-j222-j9mf-h6j9

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



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

GLPI before before version 9.4.6 has a vulnerability involving a default encryption key. GLPIKEY is public and is used on every instance. This means anyone can decrypt sensitive data stored using this key. It is possible to change the key before installing GLPI. But on existing instances, data must be reencrypted with the new key. Problem is we can not know which columns or rows in the database are using that; espcially from plugins. Changing the key without updating data would lend in bad password sent from glpi; but storing them again from the UI will work.

CVE-2020-5248 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **glpi-project** - **glpi** version **< 9.4.6**

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
Deprecate GLPIKEY usage · glpi-project/glpi@efd1446 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/glpi-project/glpi/commit/efd14468c92c4da43333aa9735e65fd20cbc7c6c
Public GLPIKEY can be used to decrypt any data · Advisory · glpi-project/glpi · GitHub	Mitigation Third Party Advisory github.com text/html	CONFIRM github.com/glpi-project/glpi/security/advisories/GHSA-j222-j9mf-h6j9

Related QID Numbers

690671 Free Berkeley Software Distribution (FreeBSD) Security Update for glpi (b3695b08-3b3a-11eb-af2a-080027dbe4b7)

Exploit/POC from Github

Proof of Concept (PoC) for CVE-2020-5248.

Known Affected Configurations (CPE V2.3)

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:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

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