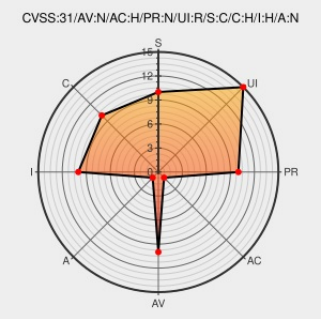
CVE-2020-15177

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

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

CVE-2020-15177 - advisory for GHSA-prvh-9m4h-4m79

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, the `install/install.php` endpoint insecurely stores user input into the database as `url_base` and `url_base_api`. These settings are referenced throughout the application and allow for vulnerabilities like Cross-Site Scripting and Insecure Redirection Since authentication is not required to perform these changes,anyone could point these fields at malicious websites or form input in a way to trigger XSS. Leveraging JavaScript it's possible to steal cookies, perform actions as the user, etc. The issue is patched in version 9.5.2.

CVE-2020-15177 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **glpi-project** - **glpi** version **>= 0.65, < 9.5.2**

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
GLPI Unauthenticated Stored XSS · Advisory · glpi-project/glpi · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/glpi-project/glpi/security/advisories/GHSA-prvh-9m4h-4m79
Merge pull request from GHSA-prvh-9m4h-4m79 · glpi-project/glpi@a8109d4 · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/glpi-project/glpi/commit/a8109d4ee970a222faf48cf48fae2d2f06465796

Related QID Numbers

690485 Free Berkeley Software Distribution (FreeBSD) Security Update for glpi (09eef008-3b16-11eb-af2a-080027dbe4b7)

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

← Previous ID

Next ID→