



CVE-2020-15176

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-15176
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-07 19:15:00 UTC
Updated	2020-10-16 15:36:00 UTC
Description	In GLPI before version 9.5.2, when supplying a back tick in input that gets put into a SQL query,the application does not escape the back tick, which can lead to SQL injection attacks.

Risk And Classification

Problem Types: CWE-89

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Glpi-project	Glpi	All	All	All	All
Application	Glpi-project	Glpi	All	All	All	All

References

Reference	Source	Link	Tags
Merge pull request from GHSA-x93w-64x9-58qw · glpi-project/glpi@f021f1f · GitHub	CONFIRM	github.com	Patch, Third Party
Multiple SQL Injections Stemming From isNameQuoted() · Advisory · glpi-project/glpi · GitHub	CONFIRM	github.com	Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[690539](#) Free Berkeley Software Distribution (FreeBSD) Security Update for glpi (b7abdb0f-3b15-11eb-af2a-080027dbe4b7)

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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