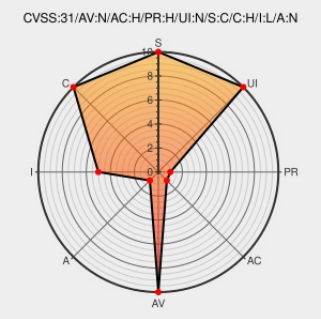
CVE-2020-11033

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

Last Modified on: 11/07/2023 03:14:00 AM UTC

CVE-2020-11033 - advisory for GHSA-rf54-3r4w-4h55

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



Certain versions of Fedora from Fedoraproject contain the following vulnerability:

In GLPI from version 9.1 and before version 9.4.6, any API user with READ right on User itemtype will have access to full list of users when querying apirest.php/User. The response contains: - All api_tokens which can be used to do privileges escalations or read/update/delete data normally non accessible to the current user. - All personal_tokens can display another users planning. Exploiting this vulnerability requires the api to be enabled, a technician account. It can be mitigated by adding an application token. This is fixed in version 9.4.6.

CVE-2020-11033 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **glpi-project** - **GLPI** version **>9.1, < 9.4.6**

CVSS3 Score: 7.2 - HIGH

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

CVSS2 Score: 6 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

CVE References

Description	Tags	Link
[SECURITY] Fedora 31 Update: glpi-9.4.6-1.fc31 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-885e2343ed
Able to read any token through API user endpoint · Advisory · glpi-project/glpi · GitHub	Vendor Advisory github.com text/html	CONFIRM github.com/glpi-project/glpi/security/advisories/GHSA-rf54-3r4w-4h55
[SECURITY] Fedora 32 Update: glpi-9.4.6-1.fc32 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-ee30e1109f

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

690673 Free Berkeley Software Distribution (FreeBSD) Security Update for glpi (aec9cbe0-3b0f-11eb-af2a-080027dbe4b7)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Glpi-project	Glpi	All	All	All	All
Application	Glpi-project	Glpi	All	All	All	All

cpe:2.3:o:fedoraproject:fedora:31:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:32:*:*:*:*:*:*:*:

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)
@LinInfoSec	Glpi - CVE-2020-11033: github.com/glpi-project/g…	2021-09-14 16:46:52

← Previous ID

Next ID→

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