# Insecure Direct Object Reference (IDOR) on "Solutions"

Moderate **trasher** published **GHSA-jvwm-gq36-3v7v** on Mar 2, 2021

Package

No package listed

| Affected versions | Patched versions |
|---|---|
| < 9.5.4 | 9.5.4 |

Description

## Impact

Ability to enumerate GLPI itemss names (including users logins) using the knowbase search form (requires authentication).

## Steps-To-Reproduce:

- Perform a valid authentication at your GLPI instance.
- Browse the ticket list and select any open ticket.
- Click on Solution form, then Search a solution form that will redirect you to the endpoint /glpi/front/knowbaseitem.php?item_itemtype=Ticket&item_items_id=18&forcetab=Knowbase$1.
- The item_itemtype=Ticket parameter present in the previous URL will point to the PHP alias of glpi_tickets table, so just replace it with "Users" to point to glpi_users table instead; in the same way, item_items_id=18 will point to the related column id, so changing it too you should be able to enumerate all the content which has an alias. For example, in our case the "admin" user is present under glpi_users table at id 8. Changing the URL accordingly like this /glpi/front/knowbaseitem.php?item_itemtype=User&item_items_id=8&forcetab=Knowbase$1 you will get the following result.

If you change the id again, you will notice that the search bar of the application will always show the information requested, so trying another item_items_id you will obtain another user id. Since such id(s) are obviously incremental, a malicious party could exploit the vulnerability simply by guessing-based attempts.

## Patches

fixed in 9.5.4

Severity

Moderate

CVE ID

CVE-2021-21324

Weaknesses

No CWEs

Credits

● indevi0us