XSS on external links in glpi-project/glpi

1

Valid Reported on Oct 3rd 2022

Description

This vulnerability allow for an administrator to create an evil external link.

Proof of Concept

As an admin user

Go to `http://172.16.128.131/front/link.form.php?id=1`

Create an external link and put has value for the link `javascript:alert(1)`

Assign this link to budgets (example)

As a regular user

Go to `http://172.16.128.131/front/budget.form.php?id=1`

Click on the *links* tab

Click on the external links

XSS triggered

Impact

This vulnerability allow an evil administrator to execute arbitrary javascript on every user that click on links.

Vulnerability Type

CWE-79: Cross-site Scripting (XSS) - Stored

Severity

Medium (4.5)

Registry

Other

Affected Version

10.0.3

Visibility

Public

Status

Fixed

Found by

w0rty

@w0rty

unranked

This report was seen 401 times.

We are processing your report and will contact the **glpi-project/glpi** team within 24 hours. 2 months ago

We have contacted a member of the **glpi-project/glpi** team and are waiting to hear back 2 months ago

A **glpi-project/glpi** maintainer has acknowledged this report 2 months ago

A **glpi-project/glpi** maintainer modified the Severity from Low (3.5) to Medium (4.5) 2 months ago

The researcher has received a minor penalty to their credibility for miscalculating the severity: -1

A **glpi-project/glpi** maintainer validated this vulnerability 2 months ago

w0rty has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

We have sent a fix follow up to the **glpi-project/glpi** team. We will try again in 7 days. 2 months ago

We have sent a second fix follow up to the **glpi-project/glpi** team. We will try again in 10 days. a month ago

We have sent a third and final fix follow up to the **glpi-project/glpi** team. This report is now considered stale. a month ago

Cédric Anne marked this as fixed in **10.0.4** with commit **01c217** 23 days ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Cédric Anne published this vulnerability 23 days ago

Sign in to join this conversation