huntr

Stored XSS in glpi-project/glpi

1

✓ Valid Reported on Sep 26th 2022

Description

openemr has a feature to customize the "Text in the login box " , due to a bad sanitization it allows to put some html tag like "form" scheme which allows to execute javascript code.

login as user glpi/glpi (admin user)
go to HOME->SETUP->GENERAL http://yoursite.com/front/config.form.php
Edit the field (Text in the login box (HTML tags supported)) and insert the payload.
logout
try the XSS.

Proof of Concept

```
PAYLOAD: <form><button formaction=javascript:alert(document.location)>click
```

Poc

Impact

The impact is JavaScript Code Execution, an attacker can steal user cretential or other things. However, admin privileges are required to edit the vulnerable input fields.

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

Severity
Medium (5.2)

Registry
Other

Affected Version

9.5.6

Visibility
Public

Status
Fixed

Found by

Hakiduck
@mike993
pro

This report was seen 445 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

Alexandre Delaunay modified the Severity from Medium (6.4) to Low (2.4) 2 months ago

Hakiduck modified the report 2 months ago

Alexandre Delaunay modified the Severity from Low (2.4) to Medium (5.2) 2 months ago

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

Alexandre Delaunay validated this vulnerability 2 months ago

Hakiduck 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

Chat with us

2 months ago

Hakiduck 2 months ago Researcher

Hi @admin, can you please assign CVE-2022-39262 to this bug ?

We have sent a second fix follow up to the **glpi-project/glpi** team. We will try again in 10 days. 2 months ago

Ben Harvie a month ago Admin

Hi Hakiduck,

I'm afraid we can only assign CVEs to reports that have been assigned by huntr.dev and not by any other CNAs.

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 **8505fb** 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