Some XSS

Moderate **trasher** published **GHSA-3g3h-rwhr-7385** on May 5, 2020

Package

glpi-project/glpi

Affected versions	Patched versions
<9.4.6	9.4.6

Description

- Stored XSS in the comments of items in the Knowledge base. Just add a comment like `<script>alert(1);</script>`.
- Self XSS via the User-Agent for administrators:

  glpi/inc/config.class.php
  Line 1836 in 7093bde

  ```
  1836    echo "\t" . $_SERVER["HTTP_USER_AGENT"] . "\n";
  ```

  . Triggered in Setup -> General -> System. Quite useless if not chained with other vulnerabilities.
- Stored XSS :
  i. Create a user with the surname `" onmouseover="alert(document.cookie)` and an empty first name.
  ii. With this user, create a ticket
  iii. As an administrator (or other privileged user) open the created ticket
  iv. On the "last update" field, put your mouse on the name of the user
  v. The XSS fires

This is difficult to tell exactly whoch versions are affected; but tha change in the Config class has been done for GLPI 0.78; we can consider all versions can be affected.

Patches

Fixed in:

- 01189af
- d45ae18
- 6dc5cb6

Reference

https://offsec.almond.consulting/multiple-vulnerabilities-in-glpi.html

For more information

If you have any questions or comments about this advisory:

- Open an issue in glpi-project/glpi
- Email us at glpi-security@ow2.org

Severity

Moderate

CVE ID

CVE-2020-11036

Weaknesses

No CWEs