The functionality add attachment to parts allows access to local files. #1229

Open **alestorm980** opened this issue on Jan 4 · 3 comments

Labels Bug needs-triage

alestorm980 commented on Jan 4

Bug description

In PartKeepr before **v1.4.0**, the functionality to load attachments using a URL when creating a part, allows the use of the **file://** URI scheme, allowing local files to be read.

Steps to reproduce

1. Go to 'Add Part'.
2. Click on 'Attachments'.
3. Click on 'Add'.
4. Fill the 'URL' field with "file:///etc/passwd".
5. Click on the uploaded file in order to see the content.

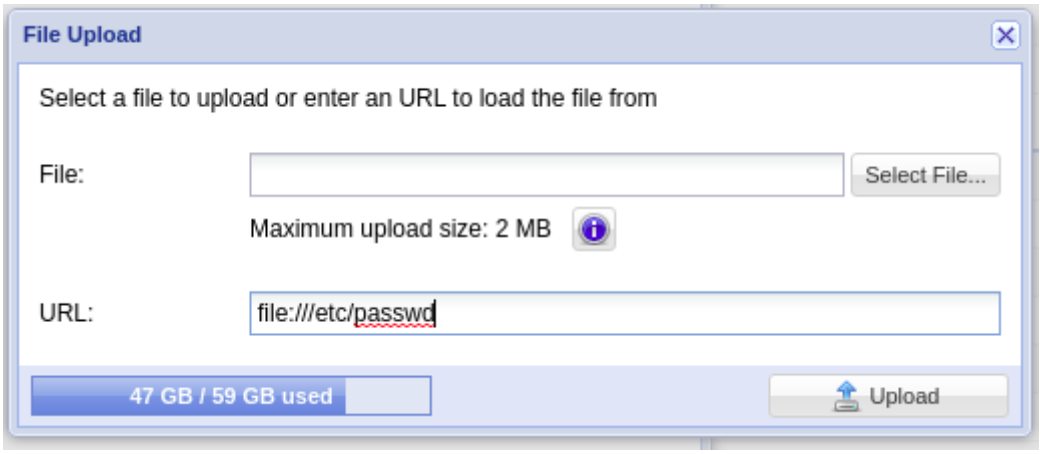
Expected behavior

The application should not allow access to local files.

Observed behavior

Local paths can be used to read files on the system.

Screenshots and files



System Information

- PartKeepr Version: v1.4.0 and v0.1.9
- Operating System: Linux
- Web Server: Apache
- PHP Version: 7.4
- Database and version: Mysql
- Reproducible on the demo system: Yes.

alestorm980 added Bug needs-triage labels on Jan 4

Gasman2014 commented on Jan 4

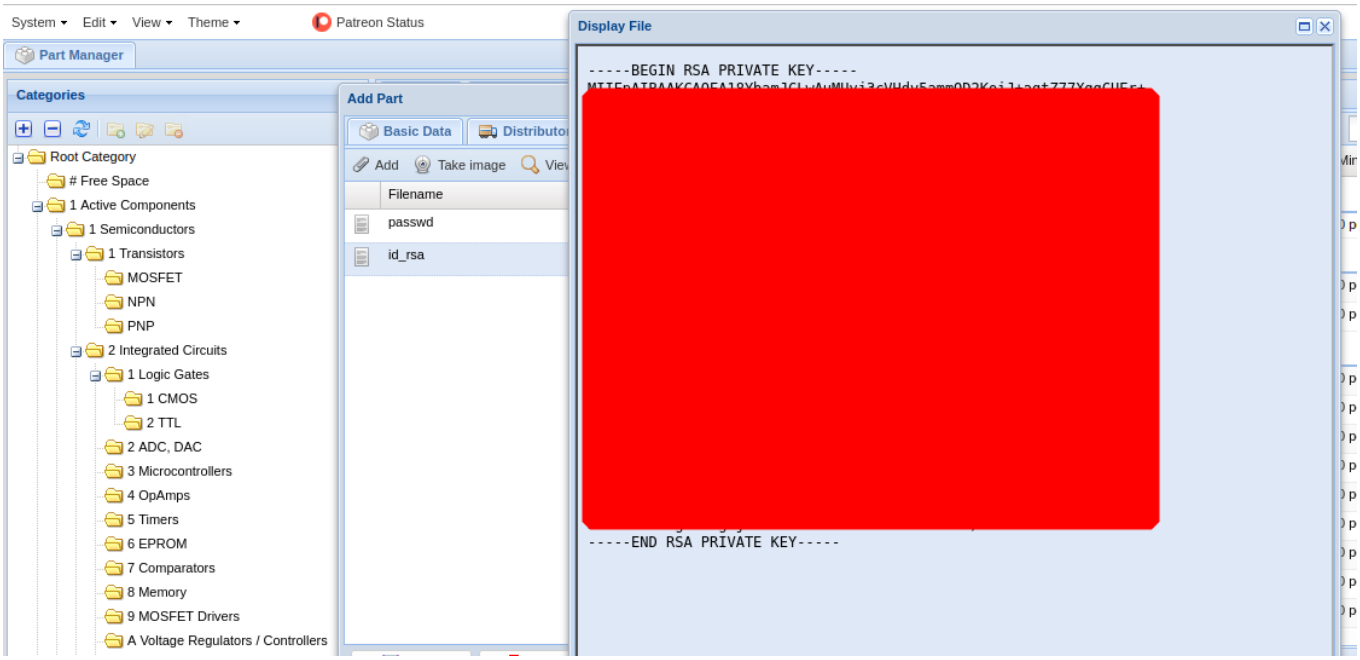
This is how most users add locally stored / downloaded data sheets / images etc. Does this allow access to resources that the user does not have permissions for?

...

alestorm980 commented on Jan 4 • edited Author

Yes, it is possible to read files within the server to which the user running the application has access, this includes source code, system configuration files, ssh keys, etc.

For example here an attacker can read a ssh key from the user running the application.



alestorm980 commented on Jan 6 — Author

I attach the link to the advisory https://fluidattacks.com/advisories/hendrix/

Assignees

No one assigned

Labels

Bug **needs-triage**

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants