

The functionality add attachment to parts allows access to local ports (SSRF). #1230



Labels

Bug

needs-triage

alestorm980 commented on Jan 4

Bug description

In PartKeepr before v1.4.0, the functionality to upload attachments using a URL when creating a part, does not validate that requests can be send to local ports, allowing SSRF attacks and port enumeration.

Steps to reproduce

- 1. Go to 'Add Part'.
- 2. Click on 'Attachments'.
- 3. Click on 'Add'.
- 4. Fill the 'URL' field with an url using a local port "http://127.0.0.1:3306".
- 5. Click on the uploaded file in order to download the file and see the content.

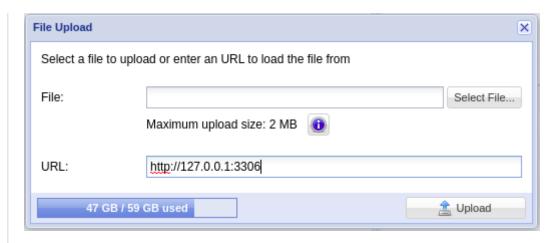
Expected behavior

The application should not allow access to local ports.

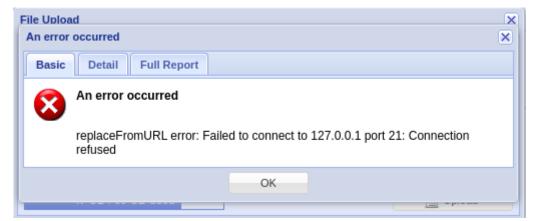
Observed behavior

Local ports can be access inside the server.

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.

а	lestorm980	com	mented	on	lan (6

Author

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

Assignees

No one assigned

Labels

Bug needs-triage

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

