DylanGrl / **CVE-2022-39833 - FileCloud RCE**

Last active 8 days ago

CVE-2022-39833 - PoC

CVE-2022-39833 - FileCloud RCE

```
Product: FileCloud

CVE: CVE-2022-39833

Version: (, 21.3.5.18513) - Tested on version 21.3.5.18513

CVSS : 9.1 - CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Vulnerability: Remote Code Execution

# Vulnerability Description :

Using the add Network Share feature, an admin is able to add a local folder instead of a
remote one. Using this feature, the admin could mount the webserver root folder and thus
access the integral code needed to run the application and modify it.

# Steps to reproduce :

1. From an administrator user, go to the Manage Network Folder location.
2. Add a new folder and choose LAN.
3. Choose a name.
4. Pick normal mount point.
5. Use /tmp as a mount point (Using webserver root here generate an error)
6. Add a normal user as allowed user.
7. Edit the Network Folder change the path for the path of the webserver root
(/var/www/html for example) and click update.
8. The Network Folder is now using the webserver root as an entry.
9. Access the folder from the normal user and confirm the possiblity to update / delete and
download all the contents from the webserver root.
10.From there, upload a PHP Shell and enjoy.
11.Sensitive information corresponding to the configuration could be retrieved as well.

Credit : GRILL Dylan
```