

YSOFT SAFEQ 6

MITIGATION GUIDE - CVE-2021-31859 AND
CVE-2022-38176

CONTENT

1	Summary	4
2	Resolution	6
2.1	Frequently Asked Questions	6
2.2	Acknowledgements	8

 **Applies to**

YSoft SAFEQ 6

Dispatcher Paragon

1 SUMMARY

This article describes how to resolve [CVE-2021-31859](#) and [CVE-2022-38176](#).

In short, this vulnerability grants members of "Authenticated users" on MS Windows the similar permissions for product folders/files as the administrators have (Write & Modify). This way, an unprivileged user can modify product executable to perform a local privilege escalation.

The list of affected products:

Operating System (OS)	Installation Location	OS Language	Product & Component	Recommendation	Note
MS Windows (client PC)	Folder inside %ProgramFiles% or %ProgramFiles(x86)%	Any	None	None	Product installed in %ProgramFiles% or %ProgramFiles(x86)% automatically inherits the set of rights that are not vulnerable to CVE-2021-31859 or CVE-2022-38176.
	Folder outside %ProgramFiles% or %ProgramFiles(x86)%	Any	YSoft SAFEQ 6 Client v3 Build 72 or older	Update to Build 74 or newer.	Tracking IDs: SBT-4146, SBT-4148, GSS-5288
			Dispatcher Paragon Client v3 Build 72 or older	Alternatively: Revoke "Authenticated users" the Write & Modify permissions. The script CVE_mitigation_script.ps1 can be used for this purpose.	
	<Drive>\<client>	Any	YSoft SAFEQ 6 FlexiSpooler Build 73 or older	Update to Build 74 or newer. Alternatively: Revoke "Authenticated users" the Write & Modify permissions. The script CVE_mitigation_script.ps1 can be used for this purpose.	
			Dispatcher Paragon FlexiSpooler Build 73 or older		

<Drive>\<folder>\<client>	English	YSoft SAFEQ 6 FlexiSpooler Build 56 or older	Update to Build 63 or newer. Alternatively: Revoke "Authenticated users" the Write & Modify permissions. The script CVE_mitigation_script.ps1 can be used for this purpose.
		Dispatcher Paragon FlexiSpooler Build 56 or older	
	Non-English	YSoft SAFEQ 6 FlexiSpooler Build 62 or older	
		Dispatcher Paragon FlexiSpooler Build 62 or older	

Timeline:

 **21 May 2021** Build 57 released fixing issue fixed for English OS and installation path <Drive>\<folder>\<client> (SBT-2655)

 **06 Dec 2021** Build 63 released fixing issue also for non-English OS and installation path <Drive>\<folder>\<client> (SBT-3319)

 **16 Aug 2022** **YSoft Quick Print** fix for v3 client MSI, v3 client installed by MSI package created after this date is no longer vulnerable (independent on v3 version, installation location, OS language) (GSS-5288)

 **22 Sep 2022** Build 73 released fixing issue for v3 client installed by CMD, PowerShell (SBT-4146)

 **07 Oct 2022** Build 74 released fixing issue for non-v3 client installed in <Drive>\<client> installed by EXE or MSI (SBT-4148)

2 RESOLUTION

Option A/ Update to the latest version if suggested in the table above.

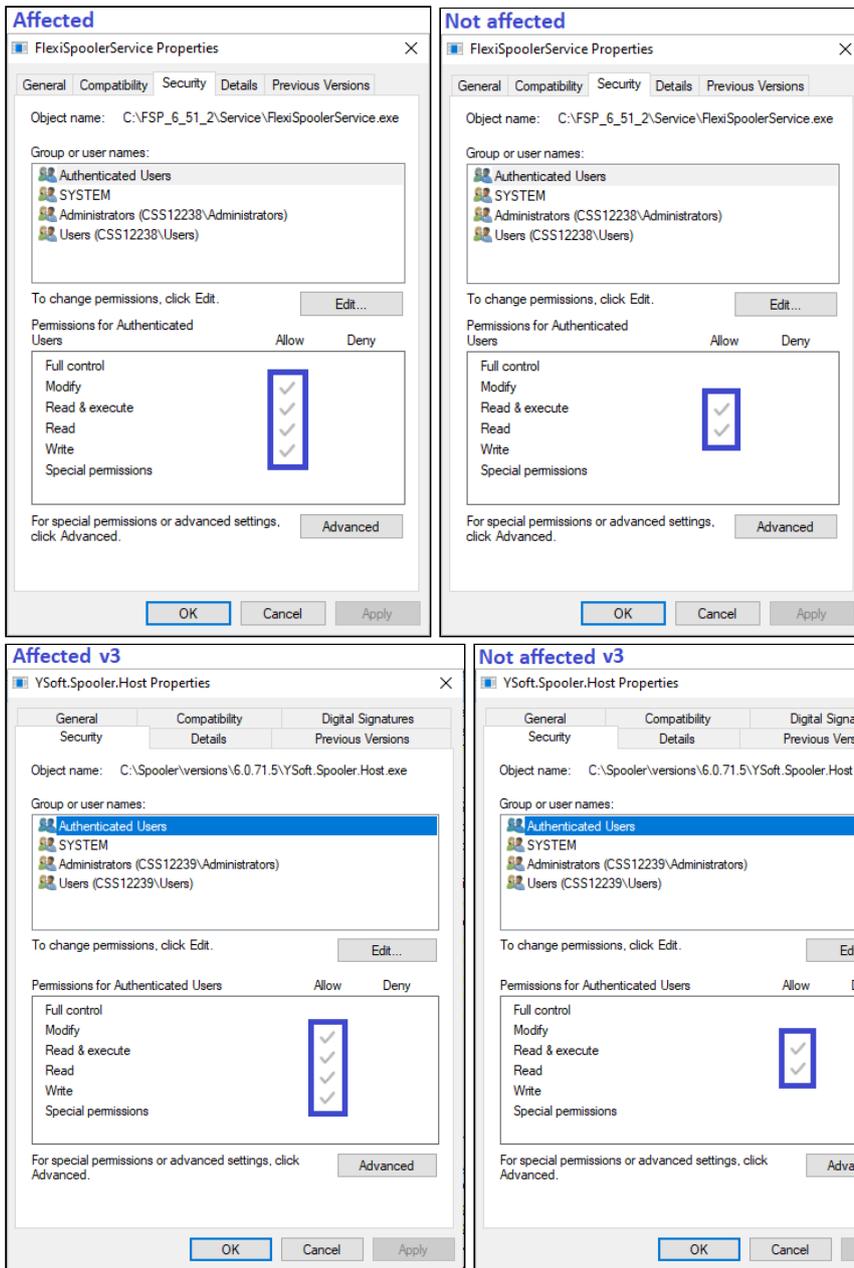
Option B/ Revoke "Authenticated users" the Write & Modify permission for the product installation directory and folders/files inside via GPO or by some other means.

Option C/ Use the script [CVE_mitigation_script.ps1](#) to revoke "Authenticated users" the Write & Modify permission for the product installation directory and folders/files inside.

2.1 FREQUENTLY ASKED QUESTIONS

Q: How can I double-check if my installation is affected?

A: See the security details for the folder and files of the component in question.



Alternatively you can use [get-acl](#) for the same purpose.

Example affected FSP

```
get-acl C:\FSP\Service\FlexiSpoolerService.exe |f
Access : NT AUTHORITY\SYSTEM Allow FullControl
BUILTIN\Administrators Allow FullControl
BUILTIN\Users Allow ReadAndExecute, Synchronize
NT AUTHORITY\Authenticated Users Allow Modify, Synchronize
```

Example not affected FSP

```
get-acl C:\FSP\Service\FlexiSpoolerService.exe |f
Access : NT AUTHORITY\SYSTEM Allow FullControl
BUILTIN\Administrators Allow FullControl
BUILTIN\Users Allow ReadAndExecute, Synchronize
NT AUTHORITY\Authenticated Users Allow ReadAndExecute, Synchronize
```

```
## Example affected v3 ##
```

```
get-acl C:\SafeQ6\Spooler\versions\6.0.71.5\YSoft.Spooler.Host.exe | fl
Access : NT AUTHORITY\SYSTEM Allow FullControl
BUILTIN\Administrators Allow FullControl
BUILTIN\Users Allow ReadAndExecute, Synchronize
NT AUTHORITY\Authenticated Users Allow Modify, Synchronize
```

```
## Example not affected v3 ##
```

```
get-acl C:\SafeQ6\Spooler\versions\6.0.71.5\YSoft.Spooler.Host.exe | fl
Access : NT AUTHORITY\SYSTEM Allow FullControl
BUILTIN\Administrators Allow FullControl
BUILTIN\Users Allow ReadAndExecute, Synchronize
NT AUTHORITY\Authenticated Users Allow ReadAndExecute, Synchronize
```

Q: Is it also safe to run the CVE_mitigation_script.ps1 on the installations that are not affected?

A: Yes, it is safe. It will cause no harm.

Q: My client is installed in C:\somefolder\FSP . After running the script, the rights for the FSP folder and files inside are fixed, but "somefolder" still has Write&Modify rights for "Authenticated Users", how is it possible?

A: You are not in direct danger and this is expected behavior. The script is only fixing the client installation directory and files inside, any folders in the path leading to it are left without any change. There are a few reasons for it:

- Explicit permissions take precedence over inherited permissions. That means even if the "Authenticated user" has Write&Modify rights on "somefolder", they still cannot alter binary files within "FSP" directory. Source:
 - <https://docs.microsoft.com/en-us/troubleshoot/windows-client/windows-security/permissions-on-copying-moving-files>
- There is no way to determine which folders in the installation path were created by the installer and which are custom made, we want to avoid modifying permissions for directories that are not our own.

Q: You are saying that only "Client PC" is affected. But I have FlexiSpooler installed on a server along with your other products. Does it mean my server is affected as well?

A: No, only the client deployed on Client PC is affected. On a server OS, the "Authenticated users" normally do not get the Write&Modify rights for every folder created on a disk drive. In addition, only the administrators can typically access the server OS, and these already have a full set of rights anyway. But you can still check the "Security" tab on any client file on the server to double-check this.

2.2 ACKNOWLEDGEMENTS

Y Soft wishes to extend its thanks to the researchers who reported these vulnerabilities:

- Remi Escourrou from Wavestone (CVE-2021-31859)
- Temuujin Darkhantsetseg from GoSecure (CVE-2022-38176)