YSOFT SAFEQ

YSOFT SAFEQ 6 CVE-2021-31859 & CVE-2022-38176 Vulnerabilities

CONTENT

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	Revoke "Authenticated users" the Write & Modify permissions. The script CVE_mitigation_script.ps1 can be used for this purpose.	Fix date in product TBA. Tracking IDs: SBT-4146, SBT-4148, GSS-5288
			Dispatcher Paragon Client v3		
	<Drive>\<client>	Any	YSoft SAFEQ 6 FlexiSpooler		
			Dispatcher Paragon FlexiSpooler		
	<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)

Pending fixes:

- SBT-4146 fix for v3 client (installation by CMD, PowerShell)
- SBT-4148 fix for non-v3 client installed in <Drive>\<client> (installation by EXE or MSI)

2 RESOLUTION

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

Option B/ Use the script CVE_mitigation_script.ps1 to revoke "Authenticated users" the Write & Modify permission for the product installation directory and folders/files inside.

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

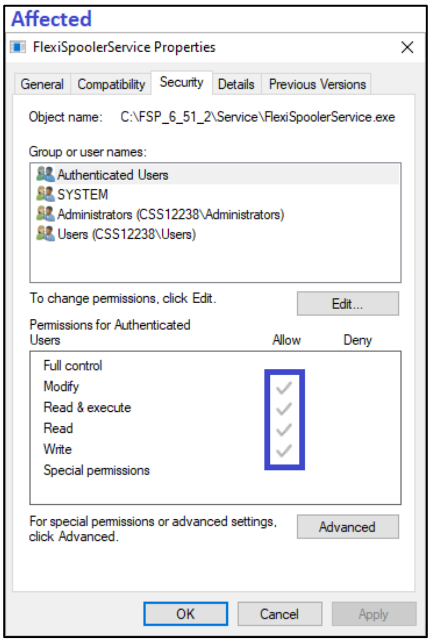
2.1 CVE_MITIGATION_SCRIPT.PS1 SCRIPT

```
<#
.SYNOPSIS
  The script for mitigating CVE-2021-31859 and CVE-2022-38176 vulnerability.

.DESCRIPTION
  The aim of script is the mitigate CVE-2021-31859 and CVE-2022-38176 vulnerability for
the following products:
    YSoft SAFEQ 6 FlexiSpooler
    YSoft SAFEQ 6 Client v3
    Dispatcher Paragon FlexiSpooler
    Dispatcher Paragon Client v3

  The script identifies product installation directory.
  The script revokes write/modify rights for "Authenticated users" for the installation
directory and all folders/files inside.

  PowerShell 3.0 or higher is required, current version can be listed by command:
$PSVersionTable.PSVersion.Major
  The script must be launched using PowerShell as an Administrator.
  Running the script multiple times on the same PC causes no harm, but it also brings no
benefit when the change is already in place.

.NOTES
  Version:        1.04
  Last Modified:  15/Jul/2022

.EXAMPLE
  Save the script as C:\Temp\CVE_mitigation_script.ps1
  Run Windows PowerShell as an administrator and launch the script as follows:
  C:\temp\CVE_mitigation_script.ps1
#>

#-----------------------------------------------------------[Execution]-------------------
-----------------------------------------

#Admin rights check
If (-NOT
([Security.Principal.WindowsPrincipal][Security.Principal.WindowsIdentity]::GetCurrent()).
IsInRole(([System.Security.Principal.SecurityIdentifier]'S-1-5-32-544'))) {
    Write-Warning 'Administrative rights are missing. Please re-run the script as an
Administrator.'
    'Press any key to exit the script.' | Out-Host
    Read-Host
    exit
}

# Function responsible for detection of product installation directory
function LocateClientdir() {
    Write-Host "Locating FSP/v3 client install directory"
    $ServiceList = @()
    $ServiceList += Get-ChildItem -Path HKLM:\SYSTEM\CurrentControlSet\Services | ? {
$_.Name -like '*YSoftSQ-FSP' -or $_.Name -like '*YSoftSQ-SPOOLER'} | Get-ItemProperty

    If ( !($ServiceList) ) {
        Throw "Client not detected, it is likely not installed. Script will be
terminated."
    }

    ForEach ($Service in $ServiceList) {
        if ( $Service.DisplayName -eq "YSoft SafeQ Spooler" ) {
            if ($Service.ImagePath -match "\w:$") {
                # Workaround for v3 client deployed by old MSI package (key ImagePath in
registry is just <drive>:, packages from QuickPrint no longer affected)
                # This detects the problematic client and updates its ImagePath inside of
source variable $ServiceList
                $tmp = $Service.ImagePath -replace
'\\\d+\.\d+\.\d+\.\d+\\..\\latest\\YSoft\.Spooler\.Host\.exe"\s--run-as-service','\latest'
-replace '"',''
            }
            else {
                $tmp = ($Service.ImagePath -replace '(?<=versions).+', '').Trim('`"')
                $tmp = $tmp.Substring(0,$tmp.LastIndexOf('\'))
            }
        }
        else {
            $tmp = $Service.ImagePath.Split()[0].Trim('`"')
            $tmp = $tmp.Substring(0,$tmp.LastIndexOf('\')) -Replace ('\\Service\\?','')
        }
        $Service | Add-Member -MemberType NoteProperty -Name Path -Value $tmp
        Write-Host "Client directory detected: $tmp"
    }
    $ServiceList.Path

}

#Functions responsible for mitigation of access rights
function SetAccessRulesForUsers($client) {
    $folderPath = $client

    Write-Host ""
    Write-Host "Getting ACL for folder [$folderPath]"
    $acl = Get-Acl $folderPath

    Write-Host "Disabling access control inheritnace from parent"
    $acl.SetAccessRuleProtection($true,$true)
    SaveAcl $acl

    $authenticatedUsers = $(New-Object System.Security.Principal.SecurityIdentifier 'S-1-
5-11').Translate( [System.Security.Principal.NTAccount]).Value
    PurgeAclRulesForAccount -Path $folderPath -Account $authenticatedUsers
    SetReadAndExecuteAclRuleForAccount -Path $folderPath -Account $authenticatedUsers

    $builtInUsers = $(New-Object System.Security.Principal.SecurityIdentifier 'S-1-5-32-
545').Translate( [System.Security.Principal.NTAccount]).Value
    PurgeAclRulesForAccount -Path $folderPath -Account $builtInUsers
    SetReadAndExecuteAclRuleForAccount -Path $folderPath -Account $builtInUsers
}

function SaveAcl() {
    param(
        $acl
    )

    Write-Host "Saving ACL"
    Set-Acl -Path $folderPath -AclObject $acl
}

function PurgeAclRulesForAccount() {
    param (
        [String] $Path,
        [String] $Account
    )
    Write-Host "Removing all access rights for account $Account"
    $ntAccount = New-Object System.Security.Principal.Ntaccount($Account)
    $acl = Get-Acl $Path
    $acl.PurgeAccessRules($ntAccount)
    SaveAcl $acl
}

function SetReadAndExecuteAclRuleForAccount() {
    param (
        [String] $Path,
        [String] $Account
    )

    Write-Host "Setting Read & Execute access rule for account $Account"

    # This combination of flags applies ACEs to "This folder, subfolders and files"
    $inheritanceFlag = 3 # https://docs.microsoft.com/en-us/dotnet/api/system.security.accesscontrol.inheritanceflags
    $propagationFlag = 0 # https://docs.microsoft.com/en-us/dotnet/api/system.security.accesscontrol.propagationflags

    $acl = Get-Acl $Path
    $accessRule = New-Object System.Security.AccessControl.FileSystemAccessRule($Account, "ReadAndExecute", $inheritanceFlag, $propagationFlag, "Allow")
    $acl.SetAccessRule($accessRule)
    SaveAcl $acl
}


$clientdir = LocateClientdir
foreach ($client in $clientdir) {
    SetAccessRulesForUsers $client
}

Write-Host ""
Write-Host "Done."
```

2.2 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.



Affected

FlexiSpoolerService Properties

Object name: C:\FSP_6_51_2\Service\FlexiSpoolerService.exe

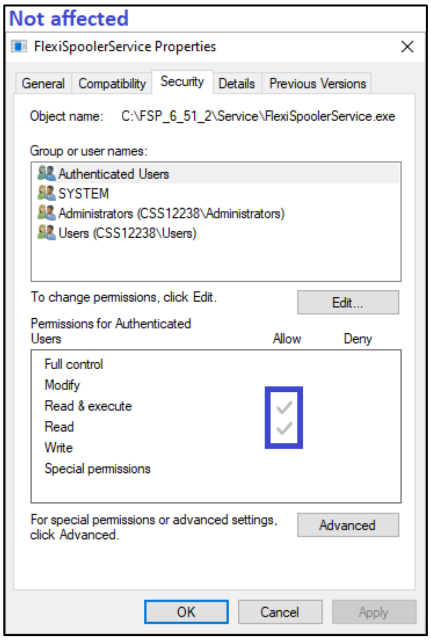
Group or user names:

- Authenticated Users
- SYSTEM
- Administrators (CSS12238\Administrators)
- Users (CSS12238\Users)

To change permissions, click Edit.

Permissions for Authenticated Users	Allow	Deny
Full control		
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

For special permissions or advanced settings, click Advanced.



Not affected

FlexiSpoolerService Properties

Object name: C:\FSP_6_51_2\Service\FlexiSpoolerService.exe

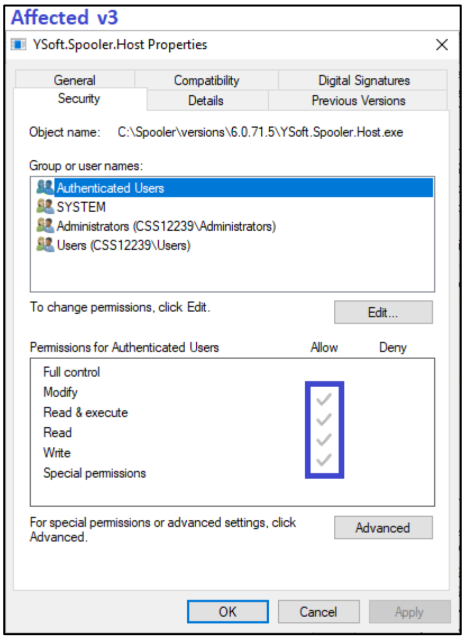
Group or user names:

- Authenticated Users
- SYSTEM
- Administrators (CSS12238\Administrators)
- Users (CSS12238\Users)

To change permissions, click Edit.

Permissions for Authenticated Users	Allow	Deny
Full control		
Modify		
Read & execute	✓	
Read	✓	
Write		
Special permissions		

For special permissions or advanced settings, click Advanced.



Affected v3

YSoft.Spooler.Host Properties

Object name: C:\Spooler\versions\6.0.71.5\YSoft.Spooler.Host.exe

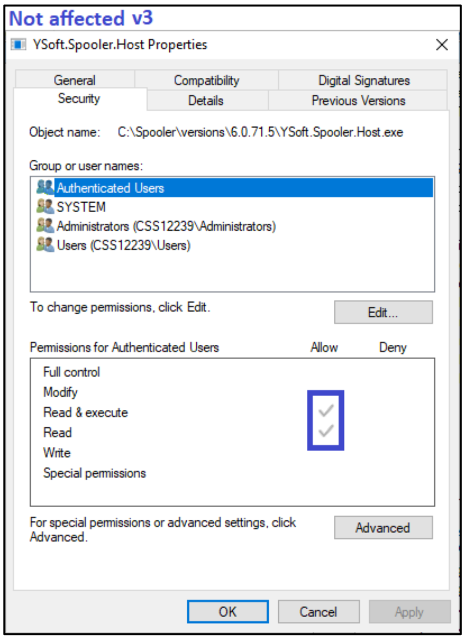
Group or user names:

- Authenticated Users
- SYSTEM
- Administrators (CSS12239\Administrators)
- Users (CSS12239\Users)

To change permissions, click Edit.

Permissions for Authenticated Users	Allow	Deny
Full control		
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

For special permissions or advanced settings, click Advanced.



Not affected v3

YSoft.Spooler.Host Properties

Object name: C:\Spooler\versions\6.0.71.5\YSoft.Spooler.Host.exe

Group or user names:

- Authenticated Users
- SYSTEM
- Administrators (CSS12239\Administrators)
- Users (CSS12239\Users)

To change permissions, click Edit.

Permissions for Authenticated Users	Allow	Deny
Full control		
Modify		
Read & execute	✓	
Read	✓	
Write		
Special permissions		

For special permissions or advanced settings, click Advanced.

Alternatively you can use get-acl for the same purpose.

```
## Example affected FSP ##
get-acl C:\FSP\Service\FlexiSpoolerService.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 FSP ##
get-acl C:\FSP\Service\FlexiSpoolerService.exe |fl
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.

2.3 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)