RICOH
imagine. change.

Microsoft ‘Print Nightmare’ Guide

v1.1

Document Revision Information

Author/Reviser	***Date***	***Version No.***	***Description***
Ricoh Technical Support Group	01/10/2021	1.0	First Release version
Ricoh Technical Support Group	01/10/2021	1.1	Added Operating Company reference

Table of Contents

Microsoft Spool Security Vulnerability ‘Print Nightmare’

Microsoft have reported security vulnerabilities linked to the Microsoft Print Spooler service. These vulnerabilities are being addressed by Microsoft with the release of security patches. This is affecting all OEM print hardware manufacturers.
Ricoh print and print management software have a dependency upon the Microsoft print service architecture. Therefore, any disruption to the Microsoft print service will have an immediate affect to your ability to print via the Ricoh supplied solution.
Ricoh therefore advise to contact Microsoft in the first instance to gain support. This document is for informational purposes. Whilst Ricoh Please distribute to your teams also.
Ricoh have no influence over the changes Microsoft have made, the following information may assist in conjunction with Microsoft’s direct advice.
Please see the following link for more information:

https://msrc-blog.microsoft.com/2021/08/10/point-and-print-default-behavior-change/

To fix the security vulnerability Microsoft have introduced the need for elevated administrator rights for users to connect to the spool service. This appears as a one-time login box when printing that requires an administrator account entered to give the rights to access and print.
For the official advice from Microsoft to work around the elevated permissions request from users please see the below information:

https://support.microsoft.com/en-us/topic/kb5005652-manage-new-point-and-print-default-driver-installation-behavior-cve-2021-34481-873642bf-2634-49c5-a23b-6d8e9a302872

Ricoh official announcement regarding the Microsoft Windows Print Spooler Vulnerability:

https://www.ricoh.co.uk/news-events/news/notice-on-microsoft-windows-print-spooler-vulnerability

Latest CVE information:

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34481

Q&A

Q. Should I disable the Spool service?
A. Ricoh print drivers and solution software require the spool service to print.

Q. Why do users get presented with a pop-up box asking for admin credentials when printing?
A. Microsoft have changed the access rights to the spool service. Elevated admin rights are now required for a connection to the spool service. This is a onetime action per user.

Q. Do the print drivers need to be upgraded?
A. No, the print drivers do not need to be upgraded. Any messages referring to driver upgrade refer to seeking admin rights to access the spooler service.

Q. I’ve been advised to reinstall print drivers, but they already reside on the clients?
A. The spooler access security changes have impacted the driver store within windows which needs the driver to be re-installed to gain permissions for the print service.

Q. Why does Windows ask for admin credentials when a user goes to print?
A. This is due to the changes Microsoft made to the spooler service in response to the security vulnerabilities. The spooler now requires elevated administrator rights when a connection is made to the service. This is a onetime action per user.

Q. How do I stop users from receiving the elevated administrator rights credentials request box from appearing when printing after the vulnerability patches have been installed?
A. Microsoft have documented a work around for this which can be found in the following link:
https://support.microsoft.com/en-us/topic/kb5005652-manage-new-point-and-print-default-driver-installation-behavior-cve-2021-34481-873642bf-2634-49c5-a23b-6d8e9a302872

Q. Can I roll out the print driver via Group Policy.
A. Yes you can, this is detailed in the following information from Microsoft:
https://support.microsoft.com/en-us/topic/kb5005652-manage-new-point-and-print-default-driver-installation-behavior-cve-2021-34481-873642bf-2634-49c5-a23b-6d8e9a302872

Q. I’ve been advised to use type 4 print drivers?
A. Type 4 drivers have worked in some situations, however these drivers have a lesser user feature experience.

Q. Can I remove the Microsoft patches to restore printing?
A. Yes, the patches can be removed from the print server. The cumulative patches for example KB5005623 have the vulnerability patches within them. These patches released on the 14th September 2021.

Q. Error 0x0000011b when printing?
A. This error can occur after the vulnerability patches are applied. Please see following link for further public domain information:
https://docs.microsoft.com/en-us/answers/questions/553928/error-0x0000011b-no-workgroup-printer-access-it-wo.html

Q. Should I have the vulnerability patches both on server and client?
A. It has been reported issues can occur if patches are not loaded both on the server and Client.

Q. Should I apply the September culminative security patches only?
A.

- January 12, 2021: Initial Deployment Phase
- September 14, 2021: Enforcement Phase

Note: if the 12th Jan 2021 updates have not been applied then the Sept 14 updates will fail to install, Use the drop down in the bulletin (link below) to see the 12th Jan 2021 updates.
https://support.microsoft.com/en-us/topic/managing-deployment-of-printer-rpc-binding-changes-for-cve-2021-1678-kb4599464-12a69652-30b9-3d61-d9f7-7201623a8b25

Useful links - Print Nightmare Information

https://www.bleepingcomputer.com/news/security/new-windows-security-updates-break-network-printing/

https://support.microsoft.com/en-gb/topic/managing-deployment-of-printer-rpc-binding-changes-for-cve-2021-1678-kb4599464-12a69652-30b9-3d61-d9f7-7201623a8b25

https://docs.microsoft.com/en-us/answers/questions/510180/how-can-we-allow-the-installation-or-update-of-the.html?page=1&pageSize=10&sort=oldest