RIMAGE®

Security Bulletin – Update

Windows Print Spooler Remote Code Execution Vulnerability

CVE-2021-34527 aka "PrintNightmare"

Microsoft has published notice of a critical vulnerability that affects all current versions of Windows. This vulnerability could allow remote code execution and privilege elevation. Currently, there is no patch to resolve this vulnerability as Microsoft is continuing to investigate.

Rimage recommends taking the additional steps below to minimize your risk while maintaining full functionality of your Rimage systems.

Install the KB5004945 patch made available by Microsoft on July 6th.

Confirm that the following registry settings are set to 0 (zero) or are not defined
(Note: These registry keys do not exist by default, if missing they are already at the secure setting and no further action is required.)

- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint
    - NoWarningNoElevationOnInstall = 0 (DWORD) or not defined (default setting)
    - UpdatePromptSettings = 0 (DWORD) or not defined (default setting)

If necessary, modify the registry keys by setting both NoWarningNoElevationOnInstall and UpdatePromptSettings as follows:

- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint
    - NoWarningNoElevationOnInstall = 0 (DWORD)
    - UpdatePromptSettings = 0 (DWORD)

More details and ongoing updates on this issue can be found on the Microsoft Security Response Center at the link below.
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527