Windows Printserver

Aufgrund der PrintNightmare-Exploits hier eine Abhandlung hinsichtlich der Serverrolle Druckserver unter Windows und wie man diese möglichst sicher betreiben kann.

Die Exploits

- CVE-2021-1675
  Remote Code Execution Vulnerability
- CVE-2021-34527 (Print Nightmare)
  Remote Code Execution Vulnerability
- CVE-2021-34481
  Elevation of Privilege Vulnerability

Einstellungen für Point-And-Print

Normalerweise sorgen die Point-And-Print-Settings dafür, dass normale Domänen-Benutzer Drucker und deren Treiber von Printservern innerhalb der Domäne nutzen, verbinden bzw. installieren können, ohne dass gesonderte Adminrechte vorhanden oder angegeben werden müssten. Dieses Verhalten ist ausnutzbar, so dass schadhafter Code getarnt als Treiber auf das System kopiert und unter Systemrechten ausgeführt werden kann.

Microsofts Lösung, welche auch durch die herausgegebenen Updates angewand wird, lautet Point-And-Print zu deaktivieren. Dies kann über folgende Registry-Keys erfolgen:

```
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)
```

Alternativ kann die Einstellung auch über GPO erfolgen.

Spooler deaktivieren oder abschotten

Kann oder möchte man auf Point-And-Print nicht verzichten, dann hilft es nur den Spooler-Dienst einschzuschränken.

Maßnahme	**Sinnvoll bei**
Spooler stoppen	Alle Systeme ohne Druckfunktion: z. B. alle Server außer **Printserver**
GPO „Disallow client connections“	Alle Systeme, die keine Drucker zur Verfügung stellen, aber selbst drucken müssen: z. B. **PCs und Notebooks sowie Terminalserver**.

Spooler deaktivieren

Hier einen Einzeiler für die Powershell (Adminrechte vorausgesetzt):

```
Stop-Service -name Spooler -force; Set-Service -name spooler -startupType disabled
```

Alternativ via GPO.

Disallow Client Connections

Computerkonfiguration → Richtlinien → Administrative Vorlagen → Drucker → [Annahme von Clientverbindungen zum Druckspooler zulassen] = **Deaktiviert**