2025/12/14 15:29 1/2 Windows Printserver

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.

Problemstellung

Leider stellt das Deaktivieren des Point-And-Print-Mechanismus die Admins eines klassischen Printserver vor eine Herausforderung: Bleibt es flächendeckend eingeschaltet, besteht enormes Kompromittierungsrisiko. Bleibt es allerdings ausgeschaltet, fragen alle Clients nach Adminrechten, sobald ein Druckertreiber installiert oder aktualisiert wird.

Spooler deaktivieren oder abschotten

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

Last update: 2021/10/26 11:52

einschzuschränken.

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

Spooler deaktivieren

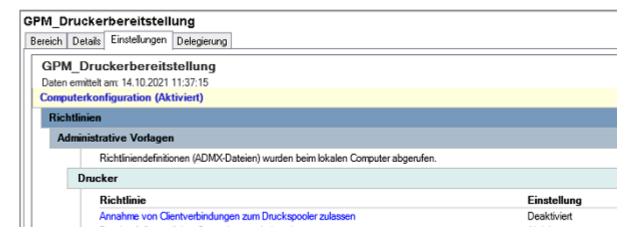
Hier einen Einzeiler für die Powershell (Adminrechte vorausgesetzt):

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

Alternativ via GPO.

Disallow Client Connections

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



From:

https://wiki.sebastianhetzel.net/ - Sebastians IT-Wiki

Permanent link:

https://wiki.sebastianhetzel.net/win_server:print?rev=1635241922

Last update: 2021/10/26 11:52

