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.

Die Lösung - der Mittelweg

Wenn wir nicht jedem Benutzer Adminrechte auf den Workstations geben möchten, bleibt nur die

Sicherheit soweit aufzuweichen, wie es nötig ist. Also teilen wir die zu schützenden Systeme in folgende Gruppen auf:

1. Domain Controller (besonders schützenswert)
2. PCs und Server ohne Printfunktion
3. PCs und Server mit Printfunktion als Client
4. Printserver

Systemrguppe	**Sinnvolle Maßnahme**
Domain Controller	Spoolerdienst deaktivieren
PCs und Server ohne Printfunktion	Spoolerdienst deaktivieren
PCs und Server mit Printfunktion als Client	GPO
Printserver	Keine Maßnahme - exponiert

Wird eine Printserverrolle auf einem Domain Controller betrieben, sollte diese schnellstens auf einen Memberserver migriert werden. Die Lücken erlauben das Erschleichen von Systemrechten auf dem Server. Ist der befallene Server ein DC, bedeutet dies, der Angreifer hat Domain-Admin-Rechte!

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**