Landespolizeipräsidium · Mainzer Straße 134-146. ·66121 Saarbrücken

Landespolizeipräsidium
LPP 2 Kriminalitätsbekämpfung/
Landeskriminalamt

Dezernat LPP 222

Dienst-gebäude: Hellwigstraße 8-10
66121 Saarbrücken

Bearbeiter_in: Schmitt M.O.KHK
Tel.: 0681 962 – 2431
Fax: 0681 962 –2445
E-Mail: cybercrime@polizei.slpol.de

Az: 25/2021

Datum: 01.07.2021

Information der
Zentralen Ansprechstelle Cybercrime (ZAC) des Landespolizeipräsidiums Saarland

Warnmeldung der zentralen Ansprechstelle Cybercrime (ZAC) Saarland hinsichtlich der Schwachstelle „PrintNightmare“ im Printer-Spooler-Service von Windows

Derzeit ist Exploit-Code in Umlauf, der an einer bislang ungepatchten Sicherheitslücke in fast allen Windows-Versionen ansetzt. **Ein Sicherheitsupdate ist bislang nicht verfügbar**.

Die betroffenen Systeme können aber mittels eines Workarounds (siehe unten) vor den Angriffen geschützt werden.

Das Problem findet sich im Printer-Spooler-Service von Windows. Dem derzeitigen Informationsstand zufolge sind davon alle Windows-Versionen von Windows 7 SP1 bis Windows 10 21H1 und Windows Server 2019 betroffen.

Laut Mitteilungen von Sicherheitsforschern kann im Erfolgsfall Schadcode mit Systemrechten ausgeführt werden. Passiert das auf einem Domain-Server, könnten Angreifer sich im Netzwerk ausbreiten und weitere Computer mit Malware infizieren.

Nach bisherigen Erkenntnissen muss ein entfernter Angreifer für eine erfolgreiche Attacke aber am System authentifiziert sein. Ist das gegeben, könnte er an der verwundbaren RpcAddPrinterDriverEx()-Funktion des Windows-Print-Spooler-Service ansetzen und dem Betriebssystem einen mit Schadcode präparierten Treiber unterschieben. Dieser wird dann mit System-Rechten ausgeführt.

Sicherheitsforscher sprechen von einem kritischen Bug.

Microsoft hat aktuell eine Warnmeldung mit weiterführenden Informationen zur Sicherheitslücke (CVE-2021-34527) veröffentlicht.

Zentrale Ansprechstelle Cybercrime (ZAC)
Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email : cybercrime@polizei.slpol.de
Web: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html

Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken

Mögliche Schutzmaßnahmen:
Administratoren sollten den Print-Spooler-Service deaktivieren, um Systeme gegen die geschilderte Attacke abzusichern.

Option 1:
Führen Sie die folgenden Befehle als Domain-Admin aus. Bitte beachten: Anschließend kann man nicht mehr lokal oder über das Netzwerk drucken.

Get-Service -Name Spooler

Wenn der Service läuft, deaktivieren Sie ihn mit den Befehlen:

Stop-Service -Name Spooler -Force
Set-Service -Name Spooler -StartupType Disabled

Option 2:
Optional können Sie den Service auch über Gruppenrichtlinien deaktivieren. Das hat den Vorteil, dass man noch lokal drucken kann. Das System fungiert aber nicht mehr als Drucker-Server.

Geben Sie dafür nach dem Druck auf die Windows-Taste "*gpedit.msc*" ein, um den Editor für die lokalen Gruppenrichtlinien aufzurufen. Unter "*Computerkonfiguration*", "*Administrative Vorlagen*", "*Drucker*" finden Sie den Punkt "A*nnahme von Client-Verbindungen zum Druckspooler zulassen*". Nach einem Rechtsklick wählen Sie "*Bearbeiten*" aus und wählen die Option "*Deaktiviert*" aus.

Option 3:
Die Exploits platzieren bösartige DLLs im Verzeichnis *C:|Windows|System32|spool|drivers.* Wenn man etwa mit ACLs dem SYSTEM-Benutzer verbietet, dieses Verzeichnis zu verändern, scheitern sie damit und das System wird nicht kompromittiert.

Die Sicherheitsfirma Truesec stellt ein kleines Powershell-Skript bereit, das diese Einstellung vornimmt. Mit diesem temporären Workaround soll sich geschützt werden können, ohne den Print-Spooler abzuschalten, erklärt die Firma in ihrem Blog-Beitrag.

Allerdings kann derzeit nicht beurteilt werden, ob das möglicherweise andere Auswirkungen hat und ob es tatsächlich langfristig schützt.

HINWEIS:
Die Benutzung der vorgenannten Optionen dient dem Schutz vor der Kompromittierung mit Schadsoftware, geschieht aber auf eigene Gefahr.

Zentrale Ansprechstelle Cybercrime (ZAC)
Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email : cybercrime@polizei.slpol.de
Web: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html

Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken

Die Polizei rät:

- Überprüfen Sie ob Sie von der aktuellen Sicherheitslücke betroffen sind.
- Deaktivieren Sie wenn möglich den Print-Spooler-Service gemäß den Optionen 1 oder 2. *Alternativ*: Prüfen Sie ob für Sie eine Nutzung des Tools von Truesec in Frage kommt.
- Überprüfen Sie in regelmäßigen Abständen ob seitens Microsoft ein Update verfügbar ist. Falls ja, updaten Sie zeitnah.

1. Quellen:

https://www.heise.de/news/PrintNightmare-Schadcode-Luecke-in-Windows-bedroht-ganze-Netzwerke-6124838.html

https://github.com/afwu/PrintNightmare

https://www.kb.cert.org/vuls/id/383432

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34527

https://blog.truesec.com/2021/06/30/fix-for-printnightmare-cve-2021-1675-exploit-to-keep-your-print-servers-running-while-a-patch-is-not-available/

Mit freundlichen Grüßen,

i.A.
KHK M.O. Schmitt
Zentrale Ansprechstelle
Cybercrime Saarland

Zentrale Ansprechstelle Cybercrime (ZAC)
Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email : cybercrime@polizei.slpol.de
Web: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html

Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken