Olympus Winter & Ibe GmbH, Kuehnstraße 61, 22045 Hamburg

An die zuständige Abteilung

Datum
30.07.2021

PrintNightmare –
Sicherheitslücke im Windows-Druckerspooler bezüglich Remotecodeausführung

Sehr geehrte Damen und Herren,

beim Windows-Druckspooler-Dienst wurde eine kritische Sicherheitslücke festgestellt. Sie hat die Bezeichnung „PrintNightmare“ erhalten. Microsoft hat dieser Sicherheitslücke die Nummer **CVE-2021-1675** zugewiesen.

Am 29. Juni 2021 begann die Verbreitung von Schadsoftware für diese Sicherheitslücke. Microsoft hat dieser Sicherheitslücke eine zweite Nummer zugewiesen: **CVE-2021-34527**.

Am 7. Juli 2021 hat Microsoft Out-of-band-Updates für einige (jedoch nicht alle) Versionen von Windows veröffentlicht. Laut der aktualisierten Empfehlung von Microsoft „enthalten am und nach dem 6. Juli 2021 veröffentlichte Sicherheitsupdates Schutzmaßnahmen für CVE-2021-1675 und für den zusätzlichen Exploit zur Remotecodeausführung im Windows-Druckerspoolerdienst, bekannt als „PrintNightmare“, der in CVE-2021-34527 dokumentiert ist.“ Eine erfolgreiche Ausführung von Exploits wurde festgestellt und ALLE Windows-Systeme sind betroffen.

Am 15. Juli 2021 hat Microsoft der PrintNightmare-Sicherheitslücke eine dritte Nummer zugewiesen: **CVE-2021-34481**. Für diese Sicherheitslücke wurde bisher kein veröffentlichter Exploit bekannt.

Betroffene OSTE Produkte

Alle Versionen der folgenden OSTE Produkte umfassen eine Version von Windows und sind von der PrintNightmare-Sicherheitslücke betroffen:

- VMC-3
- VMC-7
- VMC-10
- VMC-30.

Zum Umgang mit der PrintNightmare-Sicherheitslücke bei diesen Produkten hat OSTE das Service Bulletin SBU_100-219-293 veröffentlicht. Dieses Service Bulletin enthält Anweisungen für die Servicetechniker zum Beenden und Deaktivieren des Druckspoolerdienstes unter Windows für VMC-3, VMC-7, VMC-10 und VMC-30. Das Deaktivieren des Druckspoolerdienstes unter Windows ist eine schnelle und effektive Lösung zum Schließen der PrintNightmare-Sicherheitslücke bei Windows-Systemen.

Wenden Sie sich für eine Anwendung der im Service Bulletin definierten Abhilfemaßnahmen bei Ihrem VMC an den Olympus Kundendienst.

Weitere OSTE Produkte

OSTE entwickelt und liefert auch Software, die auf Computern mit Windows-Betriebssystem zu installieren ist:

- ENDOBASE
- Hytrack

Aufgrund des hohen Risikos der PrintNightmare-Sicherheitslücke empfiehlt OSTE dringend, die folgenden Abhilfemaßnahmen anzuwenden, um das von der PrintNightmare-Sicherheitslücke ausgehende Risiko zu minimieren.

Allgemeine Empfehlung

Von der PrintNightmare-Sicherheitslücke betroffen sind alle Windows-Versionen und alle Typen von Windows – Clients und Serverinstallationen.

Wird die Druckfunktion bei einem Windows-Computer nicht benötigt, empfiehlt OSTE das Beenden und Deaktivieren des Druckspoolerdienstes von Windows bei diesem Computer. Das Deaktivieren des Druckspoolerdienstes schließt die PrintNightmare-Sicherheitslücke bei allen Versionen und Typen von Windows. Jedoch wird hierdurch auch die Funktion zum Drucken von einem Computer deaktiviert.

Die Druckfunktion wird benötigt, um bei Hytrack Servern das automatische Drucken von Aufbereitungsprotokollen zu nutzen und um bei Hytrack Clients Protokolle manuell zu drucken.

Bei ENDOBASE Servern wird die Druckfunktion nicht benötigt.

Für die dritte CVE-Nummer im Zusammenhang mit PrintNightmare – CVE-2021-34481 – ist das Deaktivieren des Druckspoolerdienstes zum Zeitpunkt der Veröffentlichung dieses Dokuments (Juli 2021) laut Microsoft die einzige Abhilfemaßnahme.

Weitere Informationen finden Sie auf der Microsoft-Webseite für CVE-2021-34481:

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34481

Ist das Drucken von einem Windows-Computer erforderlich, hängt die empfohlene Abhilfemaßnahme von der Windows-Version ab.

Windows 10 und Windows 10-basierte Serverversionen

Microsoft hat Sicherheitsupdates für alle Versionen von Windows 10 und die zugehörigen Serverversionen veröffentlicht. Ausführliche Informationen und Links zu den entsprechenden KnowledgeBase-Artikeln finden Sie auf der Microsoft-Webseite für CVE-2021-34527:

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

Neben dem Installieren der Updates müssen Sie zum Schutz Ihres Systems sicherstellen, dass die folgenden Registrierungseinstellungen auf 0 (Null) gesetzt oder nicht definiert sind:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint`
- `NoWarningNoElevationOnInstall = 0 (DWORD) oder nicht definiert (Standardeinstellung)`
- `UpdatePromptSettings = 0 (DWORD) oder nicht definiert (Standardeinstellung)`

Wurde `NoWarningNoElevationOnInstall` auf 1 eingestellt, ist Ihr System für Angriffe anfällig konfiguriert.

Windows 7 und Windows 7-basierte Serverversionen

Für Windows 7 und Windows 7-basierte Serverversionen hat Microsoft Sicherheitsupdates nur für Kunden mit ESU-Vertrag (Extended Security Update) veröffentlicht.

Stellt das Deaktivieren des Druckspoolerdienstes keine Option dar, lässt sich das von der PrintNightmare-Sicherheitslücke ausgehende Risiko nur mithilfe einiger Workarounds minimieren.

Deaktivieren eingehender Remotedruckaufträge per Gruppenrichtlinie

Konfigurieren Sie die Einstellungen durch eine Gruppenrichtlinie wie folgt:

`Computer Configuration / Administrative Templates / Printers`

Deaktivieren Sie die Richtlinie „`Allow Print Spooler to accept client connections`“, um Remoteangriffe zu blockieren.

Damit die Gruppenrichtlinie wirksam wird, müssen Sie den Druckspoolerdienst neu starten.

Ausführliche Informationen finden Sie auf der Microsoft-Webseite für CVE-2021-34527:

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

Beschränken der Installation neuer Druckertreiber (Point-and-Print-Einstellungen)

Auch wenn kein Sicherheitsupdate installiert worden ist, werden die folgenden Einstellungen empfohlen, um das von der PrintNightmare-Sicherheitslücke ausgehende Risiko zu minimieren:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint`
- `NoWarningNoElevationOnInstall = 0 (DWORD) oder nicht definiert (Standardeinstellung)`
- `UpdatePromptSettings = 0 (DWORD) oder nicht definiert (Standardeinstellung)`

Wurde `NoWarningNoElevationOnInstall` auf 1 eingestellt, ist Ihr System für Angriffe anfällig konfiguriert.

Mit freundlichen Grüßen

Alois Baier
Product Security Manager
R&D | Product Security