

教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2021070801074040	發佈時間	2021-07-08 13:28:42
事故類型	ANA-漏洞預警	發現時間	2021-07-08 13:28:42
影響等級	中		

[主旨說明:]

【漏洞預警】【更新建議措施】微軟 Windows 列印多工緩衝處理器(Print Spooler)存在安全漏洞(CVE-2021-34527)，允許攻擊者遠端執行任意程式碼，請儘速確認並進行防護補強！

[內容說明:]

轉發 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-ANA-202107-0259

研究人員發現 Windows 列印多工緩衝處理器(Print Spooler)服務內之 RpcAddPrinterDriverEx 函式因未正確限制非授權之存取行為，導致存在安全漏洞(CVE-2021-34527)，遠端攻擊者可藉由此漏洞進而執行任意程式碼。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

[影響平台:]

受影響版本如下：

- Windows 7 for 32-bit Systems Service Pack 1
 - Windows 7 for x64-based Systems Service Pack 1
 - Windows 8.1 for 32-bit systems
 - Windows 8.1 for x64-based systems
 - Windows RT 8.1 Windows 10 for 32-bit Systems
 - Windows 10 for x64-based Systems
 - Windows 10 Version 1607 for 32-bit Systems
 - Windows 10 Version 1607 for x64-based Systems
 - Windows 10 Version 1809 for 32-bit System
 - Windows 10 Version 1809 for ARM64-based Systems
 - Windows 10 Version 1809 for x64-based Systems
 - Windows 10 Version 1909 for 32-bit Systems
 - Windows 10 Version 1909 for ARM64-based Systems
 - Windows 10 Version 1909 for x64-based Systems
 - Windows 10 Version 2004 for 32-bit Systems
 - Windows 10 Version 2004 for ARM64-based Systems
 - Windows 10 Version 2004 for x64-based Systems
 - Windows 10 Version 20H2 for 32-bit Systems
 - Windows 10 Version 20H2 for ARM64-based Systems
 - Windows 10 Version 20H2 for x64-based Systems
 - Windows 10 Version 21H1 for 32-bit Systems
 - Windows 10 Version 21H1 for ARM64-based Systems
- Windows 10 Version 21H1 for x64-based Systems
 - Windows Server 2008 for 32-bit Systems Service Pack 2
 - Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
 - Windows Server 2008 for x64-based Systems Service Pack 2
 - Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
 - Windows Server 2008 R2 for x64-based Systems Service Pack 1
 - Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
 - Windows Server 2012
 - Windows Server 2012 (Server Core installation)
 - Windows Server 2012 R2
 - Windows Server 2012 R2 (Server Core installation)
 - Windows Server 2016
 - Windows Server 2016 (Server Core installation)
 - Windows Server 2019
 - Windows Server 2019 (Server Core installation)
 - Windows Server, version 1909 (Server Core installation)
 - Windows Server, version 2004 (Server Core installation)
 - Windows Server, version 20H2 (Server Core Installation)

[參考資料:]

目前微軟官方針對此漏洞已釋出部分更新程式，除 Windows 10 version 1607、Windows Server 2012 及 Windows Server 2016 外，其餘作業系統版本均已有更新程式，請各機關聯絡設備維護廠商儘速進行更新。

尚未有更新程式之作業系統請參考以下步驟採取緩解措施，並持續留意更新程式釋出情形：

1. 透過網域主機派送群組原則物件(GPO)，或在單機電腦上執行「本機群組原則編輯器」(gpedit.msc)，將「電腦設定->系統管理範本->印表機->允許列印多工緩衝處理器接受用戶端連線」設為「已停用」。
2. 重新開機，或藉由「執行 services.msc->在 Print Spooler 服務上按右鍵->點選重新啟動」以重新啟動 Print Spooler 服務，以使設定生效。參考網址：<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527>

[參考資料:]

1. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527>
2. <https://www.ithome.com.tw/news/145427>
3. <https://kb.cert.org/vuls/id/383432>
4. <https://docs.microsoft.com/zh-tw/troubleshoot/windows-server/printing/use-group-policy-to-control-ad-printer>
5. <https://thegeekpage.com/how-to-start-stop-or-restart-print-spooler-in-windows-10/>