**張貼日期：2024/04/29**

# 【漏洞預警】Windows Print Spooler存在高風險安全漏洞(CVE-2022-38028)請儘速確認並進行修補!

- 主旨說明：【Windows Print Spooler存在高風險安全漏洞(CVE-2022-38028)】請儘速確認並進行修補!
- 內容說明:
  - 轉發 國家資安資訊分享與分析中心 NISAC-200-202404-00000102】

近期研究人員發現，特定駭客組織利用Windows Print Spooler服務之舊有漏洞(CVE-2022-38028)對外進行攻擊，由於該漏洞允許本機使用者提權至系統權限，且已遭駭客廣泛利用，請儘速確認並進行修補。

- 影響平台:
  - 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 Systems
  - Windows 10 Version 1809 for ARM64-based Systems
  - Windows 10 Version 1809 for x64-based Systems
  - Windows 10 Version 20H2 for 32-bit Systems
  - Windows 10 Version 20H2 for ARM64-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 10 Version 21H2 for 32-bit Systems
  - Windows 10 Version 21H2 for ARM64-based Systems
  - Windows 10 Version 21H2 for x64-based Systems
  - Windows 11 version 21H2 for ARM64-based Systems
  - Windows 11 version 21H2 for x64-based Systems
  - Windows 11 Version 22H2 for ARM64-based Systems
  - Windows 11 Version 22H2 for x64-based Systems
  - Windows 8.1 for 32-bit systems
  - Windows 8.1 for x64-based systems
  - Windows RT 8.1 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 2022
  - Windows Server 2022 (Server Core installation)
- 建議措施:
  - 官方已針對漏洞釋出修復更新，請參考以下網址確認修補資訊:

https://msrc.microsoft.com/update-guide/advisory/CVE-2022-38028

- 參考資料:
  1. https://msrc.microsoft.com/update-guide/advisory/CVE-2022-38028
  2. https://nvd.nist.gov/vuln/detail/CVE-2022-38028
  3. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

---

計算機與通訊中心
網路系統組 敬啟