張貼日期：2022/12/29

【漏洞預警】Linux核心存在高風險安全漏洞(CVE-2022-47939)，請儘速確認並進行更新

- 主旨說明：Linux核心存在高風險安全漏洞(CVE-2022-47939)，允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新

- 內容說明：
  - 轉發 國家資安資訊分享與分析中心 NISAC-ANA-202212-1656，
  - 研究人員發現Linux核心存在使用釋放後記憶體(Use After Free)漏洞(CVE-2022-47939)，肇因於smb2pdu.c元件處理SMB2_TREE_DISCONNECT指令過程中，未於執行指令前驗證物件是否存在，使得未經驗證之遠端攻擊者可針對已啟用ksmbd服務之Linux核心執行任意程式碼。
- 影響平台:
  - Linux Kernel 5.15至5.15.60、5.18至5.18.17及5.19至5.19.1版本
- 建議措施:
  1. 將Linux Kernel升級至5.15.61、5.18.18及5.19.2(含)以上版本。
  2. 解除安裝或停用ksmbd。
- 參考資料:
  1. https://www.ithome.com.tw/news/154880
  2. https://www.zerodayinitiative.com/advisories/ZDI-22-1690/
  3. https://cve.report/CVE-2022-47939
  4. https://nvd.nist.gov/vuln/detail/CVE-2022-47939
  5. https://www.tenable.com/cve/CVE-2022-47939
  6. https://www.openwall.com/lists/oss-security/2022/12/23/10
  7. https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.15.61
  8. https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.18.18
  9. https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.19.2

計算機與通訊中心
網路系統組 敬啟