

張貼日期：2025/03/18

## 【漏洞預警】CISA新增9個已知遭駭客利用之漏洞至KEV目錄(2025/03/03-2025/03/09)

- 主旨說明:【漏洞預警】CISA新增9個已知遭駭客利用之漏洞至KEV目錄(2025/03/03-2025/03/09)
- 內容說明:
  - 轉發 台灣電腦網路危機處理暨協調中心 TWCERTCC-200-202503-00000006
  - [CVE-2024-13161] Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability (CVSS v3.1: 9.8)  
【是否遭勒索軟體利用:未知】 Ivanti Endpoint Manager(EPM)存在絕對路徑遍歷漏洞，允許遠端未經身份驗證的攻擊者洩露敏感資訊。  
【影響平台】請參考官方所列的影響版本  
[https://forums.ivanti.com/s/article/Security-Advisory-EPM-January-2025-for-EPM-2024-and-EPM-2022-SU6?language=en\\_US](https://forums.ivanti.com/s/article/Security-Advisory-EPM-January-2025-for-EPM-2024-and-EPM-2022-SU6?language=en_US)
  - [CVE-2024-13160] Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability (CVSS v3.1: 9.8)  
【是否遭勒索軟體利用:未知】 Ivanti Endpoint Manager(EPM)存在絕對路徑遍歷漏洞，允許遠端未經身份驗證的攻擊者洩露敏感資訊。  
【影響平台】請參考官方所列的影響版本  
[https://forums.ivanti.com/s/article/Security-Advisory-EPM-January-2025-for-EPM-2024-and-EPM-2022-SU6?language=en\\_US](https://forums.ivanti.com/s/article/Security-Advisory-EPM-January-2025-for-EPM-2024-and-EPM-2022-SU6?language=en_US)
  - [CVE-2024-13159] Ivanti Endpoint Manager (EPM) Absolute Path Traversal Vulnerability (CVSS v3.1: 9.8)  
【是否遭勒索軟體利用:未知】 Ivanti Endpoint Manager(EPM)存在絕對路徑遍歷漏洞，允許遠端未經身份驗證的攻擊者洩露敏感資訊。  
【影響平台】請參考官方所列的影響版本  
[https://forums.ivanti.com/s/article/Security-Advisory-EPM-January-2025-for-EPM-2024-and-EPM-2022-SU6?language=en\\_US](https://forums.ivanti.com/s/article/Security-Advisory-EPM-January-2025-for-EPM-2024-and-EPM-2022-SU6?language=en_US)
  - [CVE-2024-57968] Advantive VeraCore Unrestricted File Upload Vulnerability (CVSS v3.1: 9.9)  
【是否遭勒索軟體利用:未知】 Advantive VeraCore存在不受限制的檔案上傳漏洞，允許遠端未經身份驗證的攻擊者通過upload.aspx將檔案上傳到非預期的資料夾。  
【影響平台】Advantive VeraCore 2024.4.2.1之前的版本
  - [CVE-2025-25181] Advantive VeraCore SQL Injection Vulnerability (CVSS v3.1: 5.8)  
【是否遭勒索軟體利用:未知】 Advantive VeraCore在timeoutWarning.asp中存在SQL注入漏洞，允許遠端攻擊者通過PmSess1參數執行任意SQL指令。  
【影響平台】Advantive VeraCore 2025.1.0(含)之前的版本
  - [CVE-2025-24993] Microsoft Windows NTFS Heap-Based Buffer Overflow Vulnerability (CVSS v3.1: 7.8)  
【是否遭勒索軟體利用:未知】 Microsoft Windows新技術檔案系統(NTFS)存在基於堆疊的緩衝區溢位漏洞，允許未經授權的攻擊者在本機執行程式碼。  
【影響平台】請參考官方所列的影響版本  
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24993>
  - [CVE-2025-24991] Microsoft Windows NTFS Out-Of-Bounds Read Vulnerability (CVSS v3.1: 5.5)  
【是否遭勒索軟體利用:未知】 Microsoft Windows新技術檔案系統(NTFS)存在越界讀取漏洞，允許未經授權的攻擊者在本機洩露資訊。  
【影響平台】請參考官方所列的影響版本  
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24991>

- □CVE-2025-24985□Microsoft Windows Fast FAT File System Driver Integer Overflow Vulnerability (CVSS v3.1: 7.8)  
【是否遭勒索軟體利用:未知□ Microsoft Windows Fast FAT檔案系統驅動程式存在整數溢位漏洞，允許未經授權的攻擊者在本機執行程式碼。  
【影響平台】請參考官方所列的影響版本  
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24985>
- □CVE-2025-24984□Microsoft Windows NTFS Information Disclosure Vulnerability (CVSS v3.1: 4.6)  
【是否遭勒索軟體利用:未知□ Microsoft Windows新技術檔案系統(NTFS)存在敏感資訊插入日誌檔案的漏洞，允許未經授權的攻擊者通過物理攻擊洩露資訊。成功利用此漏洞的攻擊者可能讀取堆記憶體的部分內容。  
【影響平台】請參考官方所列的影響版本  
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24984>
- □CVE-2025-24983□Microsoft Windows Win32k Use-After-Free Vulnerability (CVSS v3.1: 7.0)  
【是否遭勒索軟體利用:未知□ Microsoft Windows Win32核心子系統存在記憶體釋放後使用漏洞，允許經授權的攻擊者在本機提升權限。  
【影響平台】請參考官方所列的影響版本  
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24983>
- □CVE-2025-26633□Microsoft Windows Management Console (MMC) Improper Neutralization Vulnerability (CVSS v3.1: 7.0)  
【是否遭勒索軟體利用:未知□ Microsoft Windows管理控制台(MMC)存在不當中和漏洞，允許未經授權的攻擊者在本地繞過安全功能。  
【影響平台】請參考官方所列的影響版本  
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633>
- □CVE-2025-21590□Juniper Junos OS Improper Isolation or Compartmentalization Vulnerability (CVSS v3.1: 6.7)  
【是否遭勒索軟體利用:未知□ Juniper Junos OS存在不當隔離或區隔漏洞，可能允許擁有高權限的本機攻擊者注入任意程式碼。  
【影響平台】請參考官方所列的影響版本  
[https://supportportal.juniper.net/s/article/2025-03-Out-of-Cycle-Security-Bulletin-Junos-OS-A-local-attacker-with-shell-access-can-execute-arbitrary-code-CVE-2025-21590?language=en\\_US](https://supportportal.juniper.net/s/article/2025-03-Out-of-Cycle-Security-Bulletin-Junos-OS-A-local-attacker-with-shell-access-can-execute-arbitrary-code-CVE-2025-21590?language=en_US)
- □CVE-2025-24201□Apple Multiple Products WebKit Out-of-Bounds Write Vulnerability (CVSS v3.1: 8.8)  
【是否遭勒索軟體利用:未知□ Apple iOS□iPadOS□macOS及其他Apple產品在WebKit中存在越界寫入漏洞，可能允許惡意設計的網頁內容突破Web內容沙箱。此漏洞可能影響使用WebKit的HTML剖析器，包括但不限於Apple Safari及依賴WebKit處理HTML的非Apple產品。  
【影響平台】請參考官方所列的影響版本 <https://support.apple.com/en-us/122281>  
<https://support.apple.com/en-us/122283> <https://support.apple.com/en-us/122284>  
<https://support.apple.com/en-us/122285>
- 影響平台: 詳細內容於內容說明欄之影響平台
- 建議措施:
  - □CVE-2024-13161□ 官方已針對漏洞釋出修復更新，請更新至相關版本  
[https://forums.ivanti.com/s/article/Security-Advisory-EPM-January-2025-for-EPM-2024-and-EPM-2022-SU6?language=en\\_US](https://forums.ivanti.com/s/article/Security-Advisory-EPM-January-2025-for-EPM-2024-and-EPM-2022-SU6?language=en_US)
  - □CVE-2024-13160□ 官方已針對漏洞釋出修復更新，請更新至相關版本  
[https://forums.ivanti.com/s/article/Security-Advisory-EPM-January-2025-for-EPM-2024-and-EPM-2022-SU6?language=en\\_US](https://forums.ivanti.com/s/article/Security-Advisory-EPM-January-2025-for-EPM-2024-and-EPM-2022-SU6?language=en_US)
  - □CVE-2024-13159□ 官方已針對漏洞釋出修復更新，請更新至相關版本  
[https://forums.ivanti.com/s/article/Security-Advisory-EPM-January-2025-for-EPM-2024-and-EPM-2022-SU6?language=en\\_US](https://forums.ivanti.com/s/article/Security-Advisory-EPM-January-2025-for-EPM-2024-and-EPM-2022-SU6?language=en_US)
  - □CVE-2024-57968□ 官方已針對漏洞釋出修復更新，請更新至相關版本

- <https://advantive.my.site.com/support/s/article/VeraCore-Release-Notes-2024-4-2-1>
- [CVE-2025-25181] 官方已針對漏洞釋出修復更新，請更新至相關版本  
<https://advantive.my.site.com/support/s/article/Veracore-Release-Notes-2025-1-1-3>
- [CVE-2025-24993] 官方已針對漏洞釋出修復更新，請更新至相關版本  
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24993>
- [CVE-2025-24991] 官方已針對漏洞釋出修復更新，請更新至相關版本  
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24991>
- [CVE-2025-24985] 官方已針對漏洞釋出修復更新，請更新至相關版本  
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24985>
- [CVE-2025-24984] 官方已針對漏洞釋出修復更新，請更新至相關版本  
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24984>
- [CVE-2025-24983] 官方已針對漏洞釋出修復更新，請更新至相關版本  
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24983>
- [CVE-2025-26633] 官方已針對漏洞釋出修復更新，請更新至相關版本  
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26633>
- [CVE-2025-21590] 官方已針對漏洞釋出修復更新，請更新至相關版本  
[https://supportportal.juniper.net/s/article/2025-03-Out-of-Cycle-Security-Bulletin-JunOS-A-local-attacker-with-shell-access-can-execute-arbitrary-code-CVE-2025-21590?language=en\\_US](https://supportportal.juniper.net/s/article/2025-03-Out-of-Cycle-Security-Bulletin-JunOS-A-local-attacker-with-shell-access-can-execute-arbitrary-code-CVE-2025-21590?language=en_US)
- [CVE-2025-24201] 官方已針對漏洞釋出修復更新，請更新至相關版本  
<https://support.apple.com/en-us/122281> <https://support.apple.com/en-us/122283>  
<https://support.apple.com/en-us/122284> <https://support.apple.com/en-us/122285>

計算機與通訊中心  
網路系統組 敬啟

From:

<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:

[https://net.nthu.edu.tw/netsys/mailling:announcement:20250318\\_02](https://net.nthu.edu.tw/netsys/mailling:announcement:20250318_02)



Last update: **2025/03/18 14:15**