

張貼日期：2026/09/30

【漏洞預警】CISA新增7個已知遭駭客利用之漏洞至KEV目錄(2026/09/14-2026/09/20)

- 主旨說明: 【漏洞預警】CISA新增7個已知遭駭客利用之漏洞至KEV目錄(2026/09/14-2026/09/20)
- 內容說明:
 - 轉發 台灣電腦網路危機處理暨協調中心 資安訊息警訊 TWCERTCC-200-202609-00000022
 - [CVE-2026-76461]Cisco Secure Email Gateway SQL Injection Vulnerability (CVSS v3.1: 9.8)
 - 【是否遭勒索軟體利用:未知】
 - 適用於Cisco Secure Email Gateway的Cisco AsyncOS 軟體存在SQL注入漏洞，未經身分驗證的遠端攻擊者可能利用此漏洞，在底層作業系統上以root權限執行任意指令。
 - [CVE-2026-58704]Google Pixel Improper Authorization Vulnerability (CVSS v3.1: 8.8)
 - 【是否遭勒索軟體利用:未知】
 - Google Pixel 裝置的行動通訊數據機存在不當授權漏洞。此邏輯錯誤可能使攻擊者得以繞過權限檢查並提升權限。
 - [CVE-2026-76460]Cisco Identity Services Engine Incorrect Use of Privileged APIs Vulnerability (CVSS v3.1: 10.0)
 - 【是否遭勒索軟體利用:未知】
 - Cisco Identity Services Engine [ISE]和Cisco ISE Passive Identity Connector [ISE-PIC]存在不當使用特權 API漏洞，可能讓未經身分驗證的遠端攻擊者繞過Web管理介面，從而未經授權存取受影響的裝置。
 - [CVE-2026-87886]Acronis Backup Incorrect Default Permissions Vulnerability (CVSS v3.1: 7.8)
 - 【是否遭勒索軟體利用:未知】
 - Acronis Backup之cPanel & WHM 外掛程式與Plesk擴充功能存在不正確的預設權限漏洞，可能導致權限提升。
 - [CVE-2025-39964]Linux Kernel Race Condition Vulnerability (CVSS v3.1: 7.8)
 - 【是否遭勒索軟體利用:未知】
 - Linux Kernel存在條件競爭漏洞，允許對同一個AF_ALG socket進行並行寫入，導致資料以不可預期的方式交錯，並造成socket內部狀態不一致。
 - [CVE-2026-53266]Linux Kernel Out-of-Bounds Write Vulnerability (CVSS v3.1: 8.8)
 - 【是否遭勒索軟體利用:未知】
 - Linux Kernel的ebtables SNAT target中存在越界寫入漏洞。此漏洞允許對ARP發送端硬體位址重寫，直接寫入由splice匯入的檔案頁面所支援的非線性socket buffer片段。受影響的產品可能已達到產品生命週期終止[EoL]或服務終止[EoS]建議使用者停止使用受影響的產品或轉移至受支援的版本。
 - [CVE-2025-39682]Linux Kernel Improper Check for Unusual or Exceptional Conditions Vulnerability (CVSS v3.1: 9.8)
 - 【是否遭勒索軟體利用:未知】
 - Linux Kernel的TLS接收路徑存在異常或例外狀況檢查不當漏洞，允許從rx_list擷取的零長度記錄繞過預期的recvmmsg()記錄類型處理機制，可能導致後續TLS記錄在處理時採用不正確的零複製與佇列假設。受影響的產品可能已達到產品生命週期終止[EoL]或服務終止[EoS]建議使用者停止使用受影響的產品或轉移至受支援的版本。
- 影響平台:
 - [CVE-2026-76461]請參考官方所列的影響版本

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-es-a-inj-2bLVGmhX>
- [CVE-2026-58704]請參考官方所列的影響版本
- <https://source.android.com/docs/security/bulletin/pixel/2026/2026-09-01>
- [CVE-2026-76460]請參考官方所列的影響版本
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-ABP-VNSW7Tn5>
- [CVE-2026-87886]請參考官方所列的影響版本
- <https://security-advisory.acronis.com/advisories/SEC-10986>
- [CVE-2025-39964]請參考官方所列的影響版本
- <https://lore.kernel.org/linux-cve-announce/2025101334-CVE-2025-39964-7964@gregkh/>
- [CVE-2026-53266]請參考官方所列的影響版本
- <https://lore.kernel.org/linux-cve-announce/2026062517-CVE-2026-53266-6162@gregkh/>
- [CVE-2025-39682]請參考官方所列的影響版本
- <https://lore.kernel.org/linux-cve-announce/2025090545-CVE-2025-39682-ddab@gregkh/>
- 建議措施:
 - [CVE-2026-76461] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-es-a-inj-2bLVGmhX>
 - [CVE-2026-58704] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://source.android.com/docs/security/bulletin/pixel/2026/2026-09-01>
 - [CVE-2026-76460] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-ABP-VNSW7Tn5>
 - [CVE-2026-87886] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://security-advisory.acronis.com/advisories/SEC-10986>
 - [CVE-2025-39964] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://lore.kernel.org/linux-cve-announce/2025101334-CVE-2025-39964-7964@gregkh/>
 - [CVE-2026-53266] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://lore.kernel.org/linux-cve-announce/2026062517-CVE-2026-53266-6162@gregkh/>
 - [CVE-2025-39682] 官方已針對漏洞釋出修復更新，請更新至相關版本
<https://lore.kernel.org/linux-cve-announce/2025090545-CVE-2025-39682-ddab@gregkh/>
- 參考資料:

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:20260930_21

Last update: **2026/09/30 13:47**

