教育機構 ANA 通報平台

發佈編號	TACERT-ANA-20260831100835 35	發佈時間	2026-08-31 10:44:39
事故類型	ANA-漏洞預警	發現時間	2026-08-31 10:44:39
影響等級	低		

[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 (2026/08/17-2026/08/23)

[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-200-202608-00000018

【CVE-2025-62593】Ray-Project Ray Code Injection Vulnerability (CVSS v3.1: 8.8)

【是否遭勒索軟體利用:未知】 Ray-Project Ray 存在程式碼注入漏洞，可能導致遠端程式碼執行。該漏洞可透過 Firefox 和 Safari 被利用。

【CVE-2026-33824】Microsoft Internet Key Exchange (IKE) Service Extensions Double Free Vulnerability (CVSS v3.1: 9.8)

【是否遭勒索軟體利用:未知】 Microsoft Internet Key Exchange(IKE)服務擴充功能存在記憶體雙重釋放漏洞，可能導致遠端程式碼執行。

【CVE-2026-59310】Broadcom VMware vCenter Path Traversal Vulnerability (CVSS v3.1: 9.8)

【是否遭勒索軟體利用:未知】 Broadcom VMware vCenter 存在路徑遍歷漏洞，可能使具備 vCenter 網路存取權限的威脅行為者得以執行任意程式碼。

【CVE-2026-55040】Microsoft SharePoint Weak Authentication Vulnerability (CVSS v3.1: 9.1)

【是否遭勒索軟體利用:未知】 Microsoft SharePoint 存在驗證機制不足漏洞，可能使未經授權的攻擊者透過網路繞過安全性功能。

【CVE-2026-65400】Apple macOS Improper Authentication Vulnerability (CVSS v3.1: 9.8)

【是否遭勒索軟體利用:未知】 Apple macOS 存在不當驗證漏洞，可能使網路上的攻擊者無需有效憑證即可通過 Screen Sharing 驗證。

【CVE-2026-64849】MLflow Server-Side Request Forgery Vulnerability (CVSS v3.1: 9.3)

【是否遭勒索軟體利用:未知】 MLflow 存在伺服器端請求偽造漏洞，可能使攻擊者得以存取內部或雲端中繼資料服務，並取得 response_status 和 response_body。

【CVE-2026-72530】TrueConf Server Code Injection Vulnerability (CVSS v3.1: 9.0)

【是否遭勒索軟體利用:未知】 TrueConf Server 存在程式碼注入漏洞，可能讓未經授權且可透過 4307/TCP 埠存取網路的遠端攻擊者，利用特製指令碼突破隔離環境，並在主機系統上執行任意程式碼。

【CVE-2026-72529】TrueConf Server Missing Authentication for Critical Function Vulnerability (CVSS v3.1: 9.8)

【是否遭勒索軟體利用:未知】 TrueConf Server 存在關鍵功能缺乏驗證漏洞，可能讓未經授權且可透過 4307/TCP 埠存取網路的遠端攻擊者，執行任意指令碼。

【CVE-2026-73570】Zimbra Collaboration Suite (ZCS) OS Command Injection Vulnerability (CVSS v3.1: 8.9)

【是否遭勒索軟體利用:未知】 Zimbra Collaboration Suite(ZCS)存在作業系統指令注入漏洞，可能使未經身分驗證的攻擊者發送特製的 SMTP 請求，進而以 Zimbra 使用者的身分執行任意作業系統指令。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

此訊息僅發送到「區縣市網路中心」，煩請貴單位協助轉發與通知轄下各單位知悉

[影響平台:]

【CVE-2025-62593】請參考官方所列的影響版本 https://github.com/ray-project/ray/security/advisories/GHSA-q279-jhrf-cc6v

【CVE-2026-33824】請參考官方所列的影響版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33824

【CVE-2026-59310】請參考官方所列的影響版本 https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017

【CVE-2026-55040】請參考官方所列的影響版本 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55040

【CVE-2026-65400】請參考官方所列的影響版本 https://support.apple.com/en-us/100100

【CVE-2026-64849】請參考官方所列的影響版本 https://github.com/mlflow/mlflow/security/advisories/GHSA-7gwp-5pfp-969j

【CVE-2026-72530】請參考官方所列的影響版本
https://trueconf.com/blog/news/security-fixes-updates-and-advisories

【CVE-2026-72529】請參考官方所列的影響版本
https://trueconf.com/blog/news/security-fixes-updates-and-advisories

【CVE-2026-73570】請參考官方所列的影響版本
https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories

[建議措施:]

【CVE-2025-62593】 官方已針對漏洞釋出修復更新，請更新至相關版本
https://github.com/ray-project/ray/security/advisories/GHSA-q279-jhrf-cc6v

【CVE-2026-33824】 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-2026-33824

【CVE-2026-59310】 官方已針對漏洞釋出修復更新，請更新至相關版本
https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017

【CVE-2026-55040】 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-2026-55040

【CVE-2026-65400】 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/100100

【CVE-2026-64849】 官方已針對漏洞釋出修復更新，請更新至相關版本
https://github.com/mlflow/mlflow/security/advisories/GHSA-7gwp-5pfp-969j

【CVE-2026-72530】 官方已針對漏洞釋出修復更新，請更新至相關版本
https://trueconf.com/blog/news/security-fixes-updates-and-advisories

【CVE-2026-72529】 官方已針對漏洞釋出修復更新，請更新至相關版本
https://trueconf.com/blog/news/security-fixes-updates-and-advisories

【CVE-2026-73570】 官方已針對漏洞釋出修復更新，請更新至相關版本
https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories