情資主旨：

CISA 新增 14 個已知遭駭客利用之漏洞至 KEV 目錄(2026/09/07-2026/09/13)

內容說明：

【CVE-2026-75650】Adobe Commerce and Magento Improper Neutralization of Special Elements Used in a Template Engine Vulnerability (CVSS v3.1: 10.0)
【是否遭勒索軟體利用:未知】
Adobe Commerce 與 Magento Open Source 存在 Improper Neutralization of Special Elements used in a Template Engine 漏洞，可能允許攻擊者執行任意程式碼。
【影響平台】請參考官方所列的影響版本
https://helpx.adobe.com/security/products/magento/apsb26-146.html

【CVE-2026-81963】Microsoft Windows Link Following Vulnerability (CVSS v3.1: 7.8)
【是否遭勒索軟體利用:未知】
Microsoft Windows Update Stack 存在連結追蹤漏洞，允許本機攻擊者將權限提升至 SYSTEM 層級。
【影響平台】請參考官方所列的影響版本
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81963

【CVE-2026-86218】N-able N-central Static Code Injection Vulnerability (CVSS v3.1: 9.8)
【是否遭勒索軟體利用:未知】
N-able N-central 存在靜態程式碼注入漏洞，可能允許在未經身分驗證的情況下進行遠端程式碼執行。
【影響平台】請參考官方所列的影響版本
https://me.n-able.com/s/security-advisory/aArVy0000002Ld3KAE/cve202686218-preauthentication-remote-code-execution

【CVE-2026-85880】Microsoft Windows Heap-Based Buffer Overflow Vulnerability (CVSS v3.1: 7.8)
【是否遭勒索軟體利用:未知】
Microsoft Windows Advanced Local Procedure Call 存在堆積緩衝區溢位漏洞，允許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-2026-85880

【CVE-2026-19490】Citrix NetScaler Authentication Bypass Using an Alternate Path or Channel Vulnerability (CVSS v3.1: 9.8)
【是否遭勒索軟體利用:未知】
Citrix NetScaler ADC 與 NetScaler Gateway 存在可透過替代路徑或通道繞過身份驗證漏洞。當 NetScaler 設備設定為 AAA 虛擬伺服器或 Gateway（SSL VPN、ICA Proxy、CVPN 或 RDP Proxy）時，未經身分驗證的遠端攻擊者可能得以繞過身分驗證。
【影響平台】請參考官方所列的影響版本
https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696939

【CVE-2025-25249】Fortinet Multiple Products Heap-based Buffer Overflow Vulnerability (CVSS v3.1: 8.1)
【是否遭勒索軟體利用:未知】
Fortinet FortiOS、FortiSwitchManager 與 FortiSASE 存在堆積緩衝區溢位漏洞，允許攻擊者透過特製封包執行未經授權的程式碼或指令。
【影響平台】請參考官方所列的影響版本
https://fortiguard.fortinet.com/psirt/FG-IR-25-084

【CVE-2026-87491】Google Chromium V8 Out of Bounds Write Vulnerability (CVSS v3.1: 8.8)
【是否遭勒索軟體利用:未知】
Google Chromium V8 存在越界寫入漏洞，遠端攻擊者可透過特製的 HTML 頁面，在沙箱內執行任意程式碼。此漏洞可能影響多款採用 Chromium 的網頁瀏覽器，包括但不限於 Google Chrome、Microsoft Edge 及 Opera。
【影響平台】請參考官方所列的影響版本
https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html

【CVE-2026-20079】Cisco Firewall Management Center Authentication Bypass Using an Alternate Path or Channel Vulnerability (CVSS v3.1: 10.0)
【是否遭勒索軟體利用:未知】
Cisco Secure Firewall Management Center (FMC) Software 與 Cisco Security Cloud Control (SCC) Firewall Management 存在可透過替代路徑或通道繞過身份驗證漏洞，可能允許未經身分驗證的遠端攻擊者繞過身分驗證，並在受影響的設備上執行指令碼檔案，進而取得底層作業系統的 root 權限。
【影響平台】請參考官方所列的影響版本

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5JPp45V2

【CVE-2026-86060】MikroTik RouterOS Improper Neutralization of Argument Delimiters in a Command Vulnerability (CVSS v3.1: 9.8)
【是否遭勒索軟體利用:未知】
MikroTik RouterOS 存在 Improper Neutralization of Argument Delimiters in a Command 漏洞，允許攻擊者變更受信任的 RouterOS Policy Mask，進而導致權限提升。
【影響平台】請參考官方所列的影響版本
https://mikrotik.com/supportsec/september-2026-vulnerability/

【CVE-2026-67277】MikroTik RouterOS Missing Authentication for Critical Function Vulnerability (CVSS v3.1: 8.2)
【是否遭勒索軟體利用:未知】
MikroTik RouterOS 存在關鍵功能缺乏身分鑑別漏洞，可能導致 btest 服務中的核心記憶體洩露及阻斷服務。
【影響平台】請參考官方所列的影響版本
https://mikrotik.com/supportsec/september-2026-vulnerability/

【CVE-2026-84869】ConnectWise ScreenConnect Improper Privilege Management and Missing Authorization Vulnerability (CVSS v3.1: 9.9)
【是否遭勒索軟體利用:未知】
ConnectWise ScreenConnect 存在權限管理不當及授權檢查不足漏洞，可能使攻擊者在未經授權或未經主機確認的情況下，透過使用中的遠端工作階段進行檔案傳輸與執行。
【影響平台】請參考官方所列的影響版本
https://www.connectwise.com/company/trust/security-bulletins/2026-09-08-screenconnect-bulletin

【CVE-2026-42016】JFrog Artifactory Incorrect Authorization Vulnerability (CVSS v3.1: 8.1)
【是否遭勒索軟體利用:未知】
JFrog Artifactory 存在不當授權漏洞，由於系統僅驗證權杖的簽章/簽發者，而非權杖的權限範圍，可能導致權限提升攻擊。
【影響平台】請參考官方所列的影響版本
https://docs.jfrog.com/releases/docs/jfrog-security-advisories

【CVE-2026-42018】JFrog Artifactory Improper Authentication Vulnerability (CVSS v3.1: 7.5)
【是否遭勒索軟體利用:未知】
JFrog Artifactory 存在不當驗證漏洞，當匿名存取功能停用時，可能會向未經身分驗證的呼叫者回傳內部的匿名使用者權杖，進而導致敏感資源外洩。
【影響平台】請參考官方所列的影響版本
https://docs.jfrog.com/releases/docs/jfrog-security-advisories

【CVE-2026-85706】GitLab Community Edition and Enterprise Edition Path Traversal Vulnerability (CVSS v3.1: 10.0)
【是否遭勒索軟體利用:未知】
GitLab Community Edition 與 Enterprise Edition 存在路徑遍歷漏洞。由於儲存庫 Commits API 中路徑限制不當且缺少強制身分驗證機制，未經身分驗證的使用者可讀取任意檔案。
【影響平台】請參考官方所列的影響版本
https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-3-2-released/

建議措施：

【CVE-2026-75650】
官方已針對漏洞釋出修復更新，請更新至相關版本
https://helpx.adobe.com/security/products/magento/apsb26-146.html

【CVE-2026-81963】
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-2026-81963

【CVE-2026-86218】
官方已針對漏洞釋出修復更新，請更新至相關版本
https://me.n-able.com/s/security-advisory/aArVy0000002Ld3KAE/cve202686218-preauthentication-remote-code-execution

【CVE-2026-85880】
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-2026-85880

【CVE-2026-19490】
官方已針對漏洞釋出修復更新，請更新至相關版本

https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696939

【CVE-2025-25249】
官方已針對漏洞釋出修復更新，請更新至相關版本
https://fortiguard.fortinet.com/psirt/FG-IR-25-084

【CVE-2026-87491】
官方已針對漏洞釋出修復更新，請更新至相關版本
https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html

【CVE-2026-20079】
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-onprem-fmc-authbypass-5JPp45V2

【CVE-2026-86060】
官方已針對漏洞釋出修復更新，請更新至相關版本
https://mikrotik.com/supportsec/september-2026-vulnerability/

【CVE-2026-67277】
官方已針對漏洞釋出修復更新，請更新至相關版本
https://mikrotik.com/supportsec/september-2026-vulnerability/

【CVE-2026-84869】
官方已針對漏洞釋出修復更新，請更新至相關版本
https://www.connectwise.com/company/trust/security-bulletins/2026-09-08-screenconnect-bulletin

【CVE-2026-42016】
官方已針對漏洞釋出修復更新，請更新至相關版本
https://docs.jfrog.com/releases/docs/jfrog-security-advisories

【CVE-2026-42018】
官方已針對漏洞釋出修復更新，請更新至相關版本
https://docs.jfrog.com/releases/docs/jfrog-security-advisories

【CVE-2026-85706】
官方已針對漏洞釋出修復更新，請更新至相關版本
https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-3-2-released/