教育機構 ANA 通報平台

發佈編號	TACERT-ANA-20260813100804O4	發佈時間	2026-08-13 10:08:05
事故類型	ANA-漏洞預警	發現時間	2026-08-13 10:08:05
影響等級	低		

[主旨說明:]【漏洞預警】CISA 新增 6 個已知遭駭客利用之漏洞至 KEV 目錄 (2026/08/03-2026/08/09)

[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-200-202608-00000009

【CVE-2026-18556】N-able N-central Authentication Bypass Using an Alternate Path or Channel Vulnerability (CVSS v4.0: 8.2)

【是否遭勒索軟體利用:未知】 N-able N-central 存在身分鑑別繞過漏洞，攻擊者可利用替代路徑或通道來繞過驗證機制。

【CVE-2026-18577】N-able N-central Authentication Bypass Using an Alternate Path or Channel Vulnerability (CVSS v4.0: 8.2)

【是否遭勒索軟體利用:未知】 N-able N-central 存在身分鑑別繞過漏洞，攻擊者可透過替代路徑或通道繞過驗證機制，進而接管 N-central 中的帳戶。此漏洞源自於針對 CVE-2026-18556 所發布的修補程式不完整。

【CVE-2026-34486】Apache Tomcat Missing Encryption of Sensitive Data

Vulnerability (CVSS v3.1: 7.5)

【是否遭勒索軟體利用:未知】 Apache Tomcat 存在敏感資料加密缺失漏洞，攻擊者可利用此漏洞繞過 EncryptInterceptor。此漏洞可與 CVE-2025-24813 串聯利用。

【CVE-2026-9198】IBM Langflow Code Injection Vulnerability (CVSS v3.1: 9.8)

【是否遭勒索軟體利用:未知】 Langflow 存在程式碼注入漏洞，未經驗證的攻擊者可利用此漏洞，在預設的 Langflow 部署環境中實現完整的遠端程式碼執行。

【CVE-2026-63077】JetBrains TeamCity Deserialization of Untrusted Data Vulnerability (CVSS v3.1: 9.8)

【是否遭勒索軟體利用:未知】 JetBrains TeamCity 存在反序列化不受信任資料漏洞，攻擊者可透過 agent polling protocol，在未經驗證的情況下遠端執行程式碼。

【CVE-2026-8037】Progress LoadMaster Command Injection Vulnerability (CVSS v3.1: 9.6)

【是否遭勒索軟體利用:未知】 Progress LoadMaster 存在指令注入漏洞，未經驗證的攻擊者可利用多個指令端點中未經清理的輸入，在 LoadMaster 設備上執行任意指令。

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-2026-18556】請參考官方所列的影響版本 https://uptime.n-able.com/event/201522/

【CVE-2026-18577】請參考官方所列的影響版本 https://uptime.n-able.com/event/201522/

【CVE-2026-34486】請參考官方所列的影響版本 https://lists.apache.org/thread/9510k5p5zdvt9pkkgtyp85mvwxo2qrly

【CVE-2026-9198】請參考官方所列的影響版本 https://www.ibm.com/support/pages/node/7278927

【CVE-2026-63077】 JetBrains TeamCity 2026.1.3, 2025.11.7 之前的版本

【CVE-2026-8037】請參考官方所列的影響版本 https://community.progress.com/s/article/LoadMaster-Critical-Security-Bulletin-June-2026-CVE-2026-8037-CVE-2026-33691

[建議措施:]

【CVE-2026-18556】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://uptime.n-able.com/event/201522/

【CVE-2026-18577】 官方已針對漏洞釋出修復更新，請更新至相關版本 https://uptime.n-able.com/event/201522/

【CVE-2026-34486】 官方已針對漏洞釋出修復更新，請更新至相關版本
https://lists.apache.org/thread/9510k5p5zdvt9pkkgtyp85mvwxo2qrly

【CVE-2026-9198】 官方已針對漏洞釋出修復更新，請更新至相關版本
https://www.ibm.com/support/pages/node/7278927

【CVE-2026-63077】 官方已針對漏洞釋出修復更新，請更新至相關版本
https://www.jetbrains.com/privacy-security/issues-fixed/

【CVE-2026-8037】 官方已針對漏洞釋出修復更新，請更新至相關版本
https://community.progress.com/s/article/LoadMaster-Critical-Security-Bulletin-June-2026-CVE-2026-8037-CVE-2026-33691