張貼日期：2026/09/10

【漏洞預警][TLP CLEAR] 英特內DreamMaker - SQL Injection

- 主旨說明:【漏洞預警][TLP CLEAR] 英特內DreamMaker - SQL Injection

- 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-200-202609-00000007
  - 【英特內DreamMaker - SQL Injection](CVE-2026-85540)(CVSS:8.8) 已通過身分鑑別之遠端攻擊者可注入任意SQL指令讀取、修改及刪除資料庫內容。
  - 【英特內DreamMaker - Reflected Cross-site Scripting](CVE-2026-85541)(CVSS:5.4) 已通過身分鑑別之遠端攻擊者可利用惡意網站於使用者端瀏覽器執行任意JavaScript程式碼。 詳細漏洞說明請參閱「漏洞資訊」。
- 影響平台:
  - Dreammaker
- 建議措施:
  - (CVE-2026-85540) 使用 SQLBuilder 元件 針對自行開發的功能，資料庫查詢或異動功能時，建議統一使用系統既有的 SQLBuilder 元件進行 SQL 組合、參數處理及資料庫操作。 應避免直接將外部輸入資料、表單參數或 URL 參數以字串串接方式組成 SQL 指令，以降低因自行開發程式處理不當而產生SQL Injection(SQL 注入）弱點的風險。 透過 SQLBuilder 或其他具備參數化查詢機制的標準元件，可進一步強化輸入資料處理及 SQL 執行安全性，並降低應用程式受到惡意 SQL 指令注入攻擊的可能性，相關元件開發使用手冊可洽本公司客服系統。
  - (CVE-2026-85541)
  - 解決方式一：限制或停用 baServer3 若系統已更新至 2026 年 4 月以後、2026年6月以前版本，即使目前仍使用 Java Composer 2.2)可先透過 WLIST 白名單機制(WhiteList)限制 jform)baServer3 的存取來源，避免未授權使用者直接存取相關功能，相關WLIST操作文件可洽本公司客服系統。 若目前系統並無開發、維護或管理上使用 baServer3 的需求，亦可直接將)servlet/baServer3.class 進行移置、停用或重新命名。此元件移除後，原則上不影響既有系統應用程式的正常執行，但將無法再透過該 Servlet 使用其相關管理或開發功能。
  - 解決方式二：更新至 Java Composer Server 2.3 可透過以下網址確認目前伺服器端 Java Composer Server 的版本及更新日期，或者透過Java Composer啟動時顯示資訊判斷：http://server-ip/servlet/baServer3
- 參考資料:
  1. https://www.twcert.org.tw/tw/cp-132-11183-06a5e-1.html

計算機與通訊中心
網路系統組 敬啟