NCC 指導辦理「5G 軟體安全： 超前部署、迎接挑戰 — 世界資安趨勢研討會」探討確保網路軟體安全與應用的資安方案

日期：110/12/01 資料來源：國家通訊傳播委員會

隨著政府加速、加量的政策指引下，我國 5G 網路的部署日益綿密，5G 作為國家邁向數位經濟與數位社會的創新基磐角色，也日益重要與顯現。5G 為達成此一願景任務，其以開放式架構與服務為導向的設計，網路功能全面軟體化；未來我們可以期待將會有各種可能創新應用例如智慧-X (工廠、醫療、交通等) 與元宇宙應用，跑在 5G 網路上。同時，在此數位時代，整體網路與應用將會面臨更多、更嚴峻的資安風險與威脅。

國家通訊傳播委員會(NCC)為此成立國家級通訊領域軟體安全實驗室，將提供 5G 軟體系統資安分析與檢測服務，透過 Security by Design ，並符合國際實務的安全軟體開發流程與程序，協助我國 5G 業者、第三方創新服務應用開發者及物聯網設備製造商業者整備其產品資安防護能力，以確保 5G 關鍵通訊網路及未來創新應用服務之安全，並同時建立我國通訊領域軟體安全能量與能力。

110 年 11 月 25 日由 NCC 指導、電信技術中心（TTC）主辦的「5G 軟體安全：超前部署、迎接挑戰—世界資安趨勢研討會」，邀請國內學界與產業界軟體開發與軟體安全專家，共同探討如何確保軟體資安的議題與解決方案。這將是一系列研討會的開始，期能藉由研討會與業界分享如何在 5G 萬物聯網創新應用時代保障軟體及其供應鏈的安全。

研討會開幕由 NCC 孫雅麗委員代表致詞，說明 5G 安全應由目前的 5G 基礎網路安全擴展納入 5G 應用、資料及物聯網設備的安全議題。本次研討會邀請三位知名專家分享軟體開發與軟體安全相關議題：

第一場是逢甲大學資訊工程系薛念林教授以「Why is Software Design Crucial? 」為題，說明符合安全的軟體開發程序的進行步驟、各項要求及開發團隊應建立的文化。

第二場由孫雅麗委員針對軟體安全實驗室進行介紹，說明設置的目標、任務與定位、執行策略，以及分享近期軟體供應鏈攻擊的案例，尤其是對針對開源軟體與平臺的攻擊。

第三場則由台灣新思科技李思賢資深業務工程師以「Application Security Orchestration and Correlation」為題說明基於應用服務安全在軟體安全開發程序(DevSecOps)在各階段進行協作、相關分析與必要檢測(如原始碼安全檢測 SCA、動態應用程式檢測 DAST、靜態應用程式檢測 SAST、交互式應用程式安全檢測 IAST等等)、檢測工具使用情境及對軟體開發安全性的影響以及在 5G 實際應用實例。

第四場則是由中央研究院資訊科技創新中心黃意婷博士後研究學者以「Open Source Intelligence for Malicious Behavior Discovery and Interpretation」分享開放原始碼情報(OSINT)在發現惡意行為與直譯的研究經驗。

為提升國家整體 5G 環境的資訊安全，NCC 關心的不止是網路的安全，更關心運作在 5G 上面的各種創新應用都能是安全可信賴的。並希望藉由軟體安全實驗室的運作，在萬物聯網的時代，能將資安的元素納入產品軟體開發生命周期裡，讓未來臺灣所有的 5G 網路都是安全、可信賴、具韌性，5G 的創新應用與相關的產品都可以令消費者與企業安心信賴。也期盼未來能協助我國的網通製造商通過產品資安認證，開拓更多商機。