112年第4季資通安全技術報告

Quarterly Technical Report

國家資通安全研究院

National Institute of Cyber Security

目　次

圖 目 次

摘要

「第 4 季資通安全技術報告」除分析本季全球資安威脅、政府通報資安事件外，並提供相對應之資安防護建議。同時，藉由資安專題分享與資安技術研析，提供政府機關需關注之資安風險重點。

「第 4 季資通安全技術報告」分為以下 4 個章節。

●資安威脅現況與防護重點

從分析全球資安威脅現況開始，第 1 起案例為駭客鎖定關鍵基礎設施為目標，入侵水、電等產業；另一起案例為基因檢測提供業者，因受害於憑證填充(Credential Stuffing)攻擊事件致大量客戶資料外洩。

分析政府資安威脅現況，發現政府機關通報事件原因，以「非法入侵」(占 65.85%)類型為主，排除綜合類型「其他」外，其次分別為「設備問題」(占 13.66%)與「網頁攻擊」(占 5.85%)為主要通報類型。

●資安專題分享

資安專題分享主題為零信任架構近期發展現況說明與推動建議，參考美國零信任架構發展，推動我國以身分鑑別、設備鑑別及信任推斷為 3 大核心機制發展之零信任架構，持續針對我國推動零信任架構之發展提出相關精進與發展之規劃藍圖。

●資安技術研析

資安技術研析主題為微軟支援診斷工具 Follina 漏洞分析與驗證實作。漏洞雖已公告修補程式，近期於全球攻擊行動中發現駭客利用不同漏洞串聯攻擊流程後，成功入侵受害者電腦並植入木馬程式，顯示攻擊未曾有停歇之兆。

●結論

本報告透過分析全球與政府之資安事件與統計數據，了解最新資安威脅趨勢與因應之資安防護重點。資安專題分享零信任架構近期發展現況說明與推動建議，以美國公布之零信任架構、策略及原則，對照我國零信任核心架構，持續推動相關應用。此外，資安技術研析分析為微軟支援診斷工具 Follina 漏洞分析與驗證實作，藉由說明 Follina 漏洞概述與成因，並實作此漏洞攻擊手法驗證，提供修補說明與後續防範建議。

1. 資安威脅現況與防護重點

本報告藉由檢視當季國內外所發生之資安事件或議題，研析事件發生之主要原因及可能之衝擊與影響。112 年第 4 季(以下簡稱本季)探討因著網路攻擊猖獗，帶來經濟損失逐漸擴大，同時應關注關鍵基礎設施也許在資安事件統計數據占比不高，惟其後續影響不容輕忽。從事件中得知組織資安防禦措施需定期滾動式檢討，發掘可能之缺口。而年度因詐騙衍生之信任議題，更值得在未來思考應對方案，防堵因新興技術或詐騙手法翻新帶來更多偽冒行為，並能提出有效且周全之方案提升數位環境韌性。

本章節之事件與議題皆配合整理相關之資安防護重點，提供政府機關就相關資安風險或議題進行評估，並依循資安管理規範與技術防禦進行強化。

1.1 全球資安威脅現況

根據富比士(Forbes)雜誌於本(112)年第 4 季刊載文章並引用資安報告表示網路攻擊對全球經濟造成之損失至明年年底，預估將高達 10.5 兆美元。而對於明年可能遭受網路安全趨勢，包含有生成式人工智慧(AI)之挑戰、缺乏足夠之網路安全人員及物聯網網路攻擊等，其中值得關注議題有升級之網路釣魚攻擊，隨著生成式 AI 工具之發展應用，讓更多攻擊者得以從中運用更具智慧且客製之策略，同時也利用深偽技術使此類社交工程攻擊將逐漸普及化。

隨著網路詐騙活動詭譎多變且猖獗狀況下，越來越難界定網路安全邊界，包含對內部人員、供應廠商、系統環境及相關服務皆衍生信任議題。從美國辭典出版商韋氏公司(Merriam-Webster)於本年 11 月公布 112 年度代表字為「真實」(Authentic) 與日前數位發展部長於媒體訪問時分享明年之資安關鍵字為「信任」(Trust Technology)，其實都代表著因 AI 新興技術與詐騙活動盛行，造成民眾對真實性與信任之期待升高，而重新塑造具備韌性與信任之數位環境，更是現今逐漸難邁入全面數位化環境後必須戮力達成之

目標。

本季全球資安事件具指標性案例為駭客鎖定關鍵基礎設施為目標，入侵水、電等產業；另一起案例為基因檢測提供業者，因受害於憑證填充(Credential Stuffing)攻擊事件致大量客戶資料外洩。

首先，探討案例關鍵基礎設施遭駭客鎖定為入侵目標，企圖影響社會秩序與安全事件，美國網路暨基礎設施安全局(Cybersecurity and Infrastructure Security Agency, CISA)發出警訊，入侵者正透過侵入暴露於公眾網上之 Unitronics 可編程邏輯控制器(Programmable Logic Controller, PLC)，試圖破壞美國之供水設施。根據媒體報導，位於賓州水務局遭到中東國家支持之網路駭客組織 CyberAv3ngers 攻擊，CyberAv3ngers 為一活躍之駭客組織，過往專門鎖定以色列水處理供應站，在這一波攻擊活動中主要對象針對以色列與美國等多處供水站。

當局發現此團體從此次入侵活動中已能控制為賓州水務局管理範圍內 2 個城鎮提供服務之遠端加壓站。惟因攻擊活動觸發警訊通知，經即時回應處理後，內部評估不論是對供水或飲用水現況皆安全無虞。且事件發生當下，系統已緊急停用並改為手動操作。據媒體報導，受感染之設備為 Unitronics PLC 設備，屬於工控環境中甚為關鍵之控制與管理設備。駭客藉由取得控制權，能透過遠端操控設備，進而變更投入之化學劑量而造成供水污染，其他風險包含中斷服務致供水中斷，以及水泵超載或開關閥門，對基礎設施直接造成實體損壞。此資安事件仍持續調查中，據初步評估駭客並非利用產品可能之零日漏洞，而是透過 Unitronics PLC 人機介面(Human Mmachine Interface, HMI)不良之設定造成，如暴露於公眾網路或弱密碼為可能肇因。

第 2 起案例為基因檢測提供業者 23andMe 因大規模資料外洩，在美國面臨多起集體訴訟，據媒體揭露共影響數百萬位客戶。入侵成功後駭客將一份

由 23andMe 命名為「Ashkenazi DNA Data of Celebrities.csv」客戶資料公布於駭客論壇，內容包含將近百萬德系猶太人有關使用 23andMe 服務尋找其祖先資訊與遺傳傾向等資料。

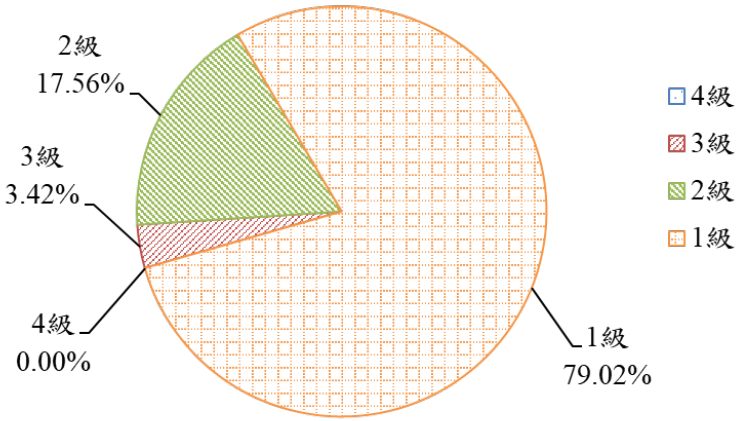
被公開資料尚包含有關 23andMe 使用者的帳戶、姓名、性別、出生日期、DNA 設定檔及地區等，且該名駭客原本採取將機敏資料曝光策略，之後改絃易轍收回檔案決定出售所竊之資料，然而當下已有其他已下載檔案之惡意人士繼續於其他社群分享，無法避免資料繼續洩露。23andMe 調查事件後發現是因為有駭客使用憑證填充攻擊，進而以獲得之合法權限存取該平台，且因該外洩資料檔未與其他檔案做好完善之權限存取原則，致連結至更多資料檔案。許多客戶認為已使用雙重驗證，並使用唯一可識別與具複雜度之密碼，卻仍發現資料遭外洩，因此決定對該公司提起團體訴訟。

綜覽本季全球資安威脅與資安事件，針對關鍵基礎設施之攻擊從未停歇，這也是為何行政院國家資通安全會報本年所辦理之大規模跨國攻防演練針對水資源領域做為攻防模擬之演練場域，研析全球工控系統發生之資安事件，再強化我國對於相關設施之防護韌性。由第 2 起事件發現若組織一味強調防護機制，卻未檢視機制之有效性，可能產生百密一疏之風險。而憑證填充之攻擊隨著運用殭屍網路或其他自動化方式操作入侵方式，將使組織遭遇更多詐騙或資料外洩事件。因此，應教育使用者培養基本良好之帳號密碼行為，避免在不同網路服務平台使用相同之帳密組合。

1.2 政府資安威脅現況

彙整本季所接獲之政府機關通報事件，藉由事件之影響等級、通報類型及事件原因，了解目前政府機關之資安威脅現況。通報事件依「機密性」、「完整性」、「可用性」3 個面向所造成之衝擊，將事件影響等級由輕至重分為 1 級、2 級、3 級及 4 級。彙整事件影響等級，本季以 1 級事件占 79.02%為大宗，2 級事件占 17.56%次之，3 級事件僅占 3.42%，而 4 級通

報事件則未發生，相關統計情形詳見圖 1。

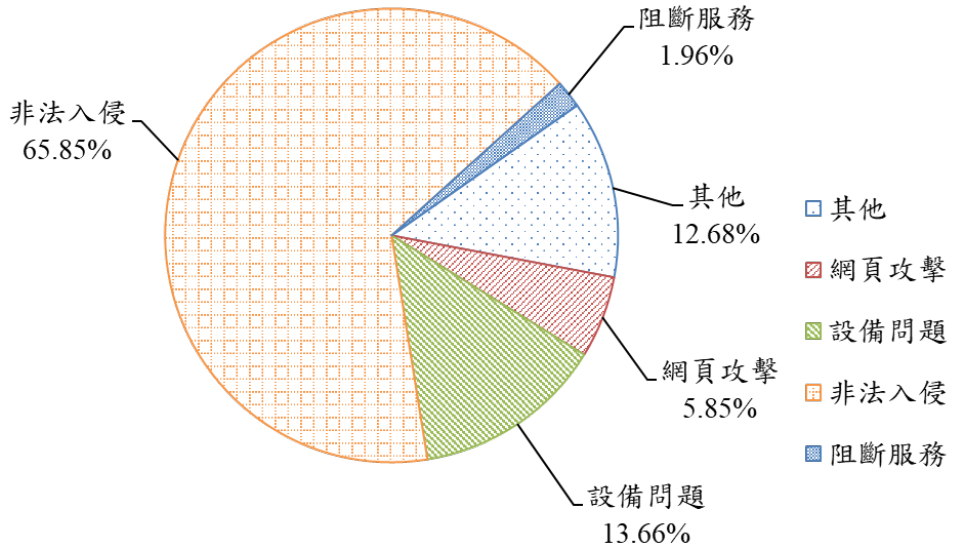


資料來源：本報告整理

圖1　112 年第 4 季通報事件影響等級比率圖

本季接獲之重要通報事件，大部分為個資外洩事件，如由民眾反映其上傳之活動個人資料或因機關查詢機主機系統遭入侵，可於 Google 搜尋引擎、社群媒體獲取或意外遭公開；另有事件案例是由國內弱點通報平台揭露因政府機關活動平台有目錄洩露漏洞，透過漏洞則可取得相關個資，這些事件皆因涉及敏感資訊外洩，故通報為 3 級資安事件。

整體通報事件類型，以「非法入侵」(占 65.85%)類型為主，排除綜合類型「其他」外，「設備問題」與「網頁攻擊」類型次之，詳見圖 2。



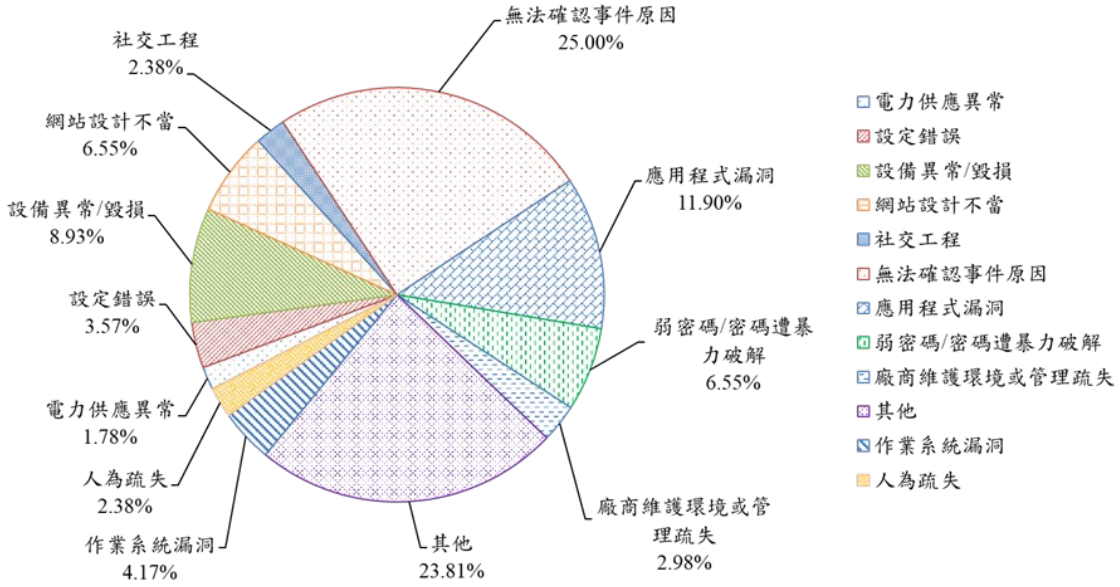
資料來源：本報告整理

圖2　112 年第 4 季通報類型比率圖

分析通報事件原因以無法確認事件原因(25%)為主，其次分別為其他(23.81%)、應用程式漏洞(11.9%)、設備異常/毀損(8.93 %)、網站設計不當(6.55%)、弱密碼/密碼遭暴力破解(6.55%)、作業系統漏洞(4.17 %)、設定錯誤(3.57%)、廠商維護環境或管理疏失(2.98 %)、社交工程(2.38 %)、人為疏失(2.38 %)及電力供應異常(1.78 %)，詳見圖 3。舉本季「社交工程」事件為例，發現惡意人人士善於利用時事議題增加郵件之真實性，以日本民間公司之電子郵件帳號，以時事日本核廢水排放議題為相關主旨，寄送夾帶惡意壓縮檔之社交工程電子郵件，針對我國政府機關進行社交工程郵件攻擊。駭客預先將惡意壓縮檔案上傳至匿名文件託管服務，再將下載連結與惡意壓縮檔附於惡意郵件，若使用者點擊附件後，將觸發批次執行檔，並成功連線至惡意中繼站。

無法歸類於系統預設事件發生原因項目者，以「其他」進行結報，本季發生因火災致系統中斷、使用者因疏失下載來源不明之應用程式及系統容量不足未能即時回應致服務中斷等事。至於「無法確認事件原因」2 大主因

為無相關紀錄檢視與逕行重建無法調查，相關日誌紀錄因被抹除或因日誌留存時間過短無法成功追溯，且有時因為服務可用性之需求，需儘快重建系統，皆造成後續無法鑑識之後果。



資料來源：本報告整理

圖3　112 年第 4 季資安事件發生原因比例圖

分析第 4 季通報類型與通報事件發生原因，排除其他與無法確認事原因類別後，應用程式漏洞為排名第 3 位之通報事件。發生案例包含部分機關資通系統使用之應用程式存在漏洞，並遭利用入侵系統，或是系統功能模組使用之元件存在高風險漏洞，致駭客透過漏洞遠端執行程式碼。

1.3 資安防護重點

分析本季全球資安威脅現況，機敏資料外洩與詐騙事件仍頻傳，可預見因網路攻擊對全球經濟造成之損失越加一發不可收拾，面對新興科技可能衍生之之攻擊樣態，惟有積極應對且預做準備，方能制敵機先。另外，關鍵基礎設施，尤其是水、電、油等，對國家、社會之安全影響重大，藉由關注國際事件與平時攻防演練，得以了解特定駭侵團體之攻擊手法，則可模

擬其入侵與預擬應變方式。對於帳密管理一直為資安防護宣導重點，也可見使用強密碼與雙重驗方式逐漸普及，惟仍可從資安事件看出或有千慮一失之處。因此對於不同攻擊手法，如憑證填充攻擊或雙驗證機制失效，仍應從置高點採滾動式策略檢視資安防護作為或方案是否有缺失。

國內部分資安事件以設備異常/毀損、社交工程、應用程式漏洞或網站設計不當為發生非法入侵或設備問題等主要肇因。以社交工程或憑證填充攻擊為例，也許風險評估後最大影響因素皆在人員之資安認知不足，社交工程來源可能來自於社群媒體、即時通訊、會議邀請連結或更多是來自於電子郵件。面對諸多社交工程攻擊情境，更應於不同面向強化防護韌性。因此對個人憑證之管理責任在於不使用同樣帳密組合於不同資訊平台，而組織則應考量面對眾多使用者在資安概念參差不一時，如何保護所管理之帳密外洩與強化驗證機制則為首重要務。

綜整以上資安威脅現況，提供資安防護建議如下：

●工控系統之資安管理

– 制定安全存取工控系統之安全組態策略，包含是否需要開放遠端存取，並識別環境中可直接連接到互聯網或其他不受信任網路之所有PLC，定期備份組態設定，以便在遭受攻擊時能快速回復。

– 訂定網路區隔與安全防護與依角色存取之控制機制(Role Based Access Control, RBAC)，避免使用預設通訊埠，並監控異常行為。

– 變更預設或弱密碼，且設計多重身份驗證，定期檢查元件或韌體之更新狀況，確保使用安全版本。

●憑證填充攻擊手法之資安管理

– 評估導入無密碼認證技術或使用雙重認證機制，惟應搭配與帳號連結之通訊設備以解鎖登入，而非可能同遭憑證攻擊社群服務平台提供之

電子郵件帳號。

– 輔助使用適切且創新之人機驗證(Captcha)方式，以提升識別能力避免遭新興科技破解或自動輸入。

– 系統設置登入失敗逾一定次數後，限制可再登入之間隔時間，同時監控網路流量，留意異常登入狀況。

2. 資安專題分享_零信任架構近期發展現況說明與推動建議

零信任為媒體選為近年最熱門資安趨勢之一，受到高度關注且帶來普世應用之風潮。零信任概念之所以蔚為風行，源自於偽冒與詐騙情況升溫，再加上遠距工作需求與 AI 等新興科技之推波助瀾因素影響下，皆使零信任應用需求勢在必行。因此世界各國均開始積極發展與推動，其中，美國針對零信任架構已發布一系列公開參考指引，而我國政府亦有相關推動措施，逐步推動零信任架構之導入。

不論是政府機關或企業要導入零信任將面臨諸多挑戰，包含環境邊界不斷地擴張、眾多且複雜之存取角色、多樣資訊設備，如物聯網、行動式設備及生物辨識系統等及廣泛之應用平台與環境，如前後台管理、內外網段、雲端及邊緣運算等等，同時若需成功導入，包含管理階層之承諾與支持，使用者改變現行使用模式之心態調整，亦應納入考量範圍。

面對許多需要解決且艱難之議題，本報告將針對美國所發布之零信任架構相關參考指引進行研析，說明其發展現況與推動情形，並進一步對我國推動現況提出建議，俾政府機關與組織導入時能有所依循。

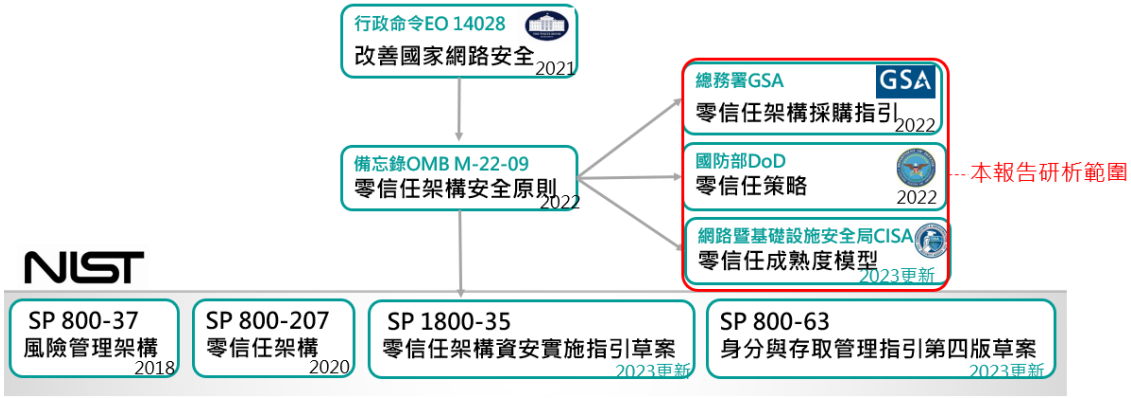
2.1 美國零信任架構發展現況

美國推動零信任架構緣自於 110 年拜登總統之行政命令(EO14028)，主要目的在改善國家網路安全，行政命令中提及網路安全現代化面向，建議聯邦政府必須採用之安全最佳實務，包含採取零信任架構與加速轉向雲端安全服務及集中並簡化對網路安全資料之存取，以推動分析、識別及管理網路安全風險。

行政命令就零信任架構，要求各機關負責人應制定實施零信任架構的計劃，於計畫中納入國家標準暨技術研究院(National Institute of Standards and

Technology, NIST)所發表之標準與指南中描敘之實施步驟，識別零信任活動可能對安全產生之立即衝擊與相關部會應提出之方案。NIST 與零信任較相關之標準則有 NIST SP 800-37 資訊系統與組織之風險管理架構、NIST SP 800-207 零風險架構系列，強調零信任之目標在於防範對資料服務發生未經授權之存取，同時將存取措施細化，以強化存取控制機制、NIST SP 1800-35 零信任架構資安實施指引草案及 NIST SP 800-63 身分與存取管理指引第四版草案。

接續總統執行辦公室(Executive of Office of the President)之管理與預算部門(Office of Management and Budget)於 111 年公布零信任架構安全原則，發展出總務署(General Services Administration, GSA)之信任架構採購指引與國防部(Department of Defense, DoD)之零信任策略及網路暨基礎設施安全局(CISA)之零信任成熟度模型。整體美國推動零信任法遵與參考文件，詳見圖 4。

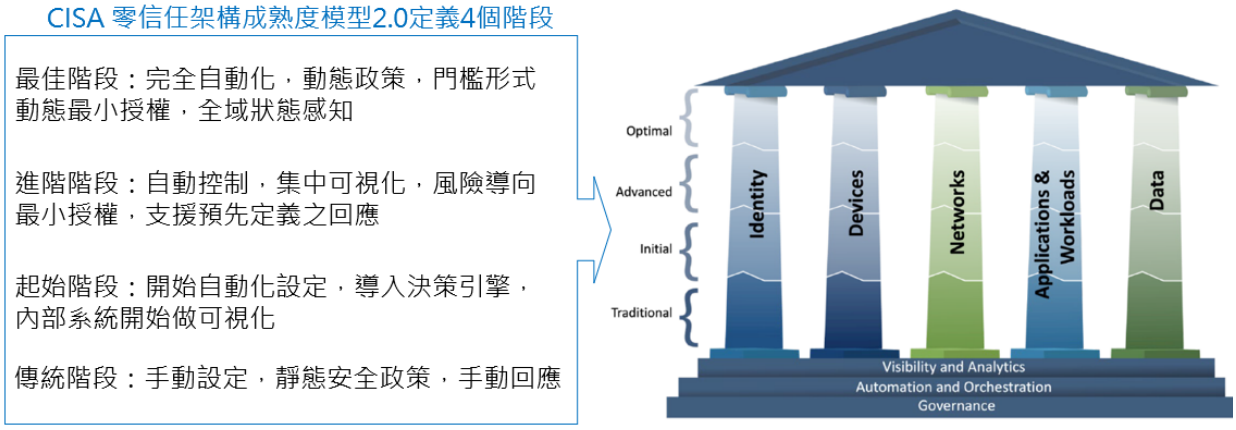


資料來源：本報告整理

圖4　美國推動零信任法遵與參考文件

首先說明零信任成熟度模型之各階段與面向，國家安全電信諮詢委員會(National Security Telecommunications Advisory Committee, NSTAC)將零信任定義為「一種網路安全策略，前提是任何使用者或資產都不應被隱喻為可被信任之標的。應假設為很可能已經發生或即將發生違規行為，因此，

不應透過在組織邊界以單一驗證授予使用者存取敏感資訊之權限。相反地，每個用戶、設備、應用程式及交易都必須持續驗證」。而 112 年 4 月 CISA 發布零信任架構成熟度模型 2.0，便由 5 個能力支柱之代表面向，分別為身分、裝置、網路、應用程式與工作負載及資料，驗證是否具備可信賴之存取權限，整體模型，詳見圖 5。



資料來源：CISA、本報告整理

圖5　成熟度模型 2.0

從成熟度模型可以得知，在 5 個能力支柱下，有 3 個跨領域之運作活動，主要在支持跨支柱與模型之整合，分別為可視化與分析，藉由組織整體環境與特性觀察與分析，協助決策與積極回應事件；自動化與協作，利用自動化工具與工作流程，支援跨產品與服務之安全回應，同時維護相關功能、產品及服務等發展過程之監督、安全性及互動；最後則為治理，負責定義於支柱內部與跨支柱之網路安全政策、程序及流程與執行，以支持零信任原則、降低風險。

CISA 零信任架構成熟度模型於 112 年公布 2.0 版本，對比 110 版本差異處，不僅成熟度導入與評估階段，且將原本傳統、進階及最佳化等 3 階細分增加初始(Initial)階段一階，同時針對 5 個能力柱，更加精準區分主題能

力之要求。CISA 零信任架構成熟度模型從導入新增之初始階段，要求開始進行屬性配置、生命週期組態、策略決策與執行之自動化，包含與外部系統整合之初始跨支柱解決方案。而在識別(Identity)功能支柱則新增存取管理於不同成熟度階段要求存取權限之持續審查與驗證，詳見圖 6。

CISA Zero Trust Maturity Model 1.0 Stages	CISA Zero Trust Maturity Model 2.0 Stages
Traditional	Traditional
	Initial
Advanced	Advanced
Optimal	Optimal

CISA Zero Trust Maturity Model 1.0 Pillars	CISA Zero Trust Maturity Model 2.0 Pillars
Identity	Identity
Device	Devices
Network / Environment	Networks
Application Workload	Applications & Workloads
Data	Data

CISA Zero Trust Maturity Model 1.0 Identity Functions	CISA Zero Trust Maturity Model 2.0 Identity Functions
Authentication	Authentication
Identity Stores	Identity Stores
Risk Assessment	Risk Assessments
	Access Management
Visibility and Analytics Capability	Visibility and Analytics Capability
Automation and Orchestration Capability	Automation and Orchestration Capability
Governance Capability	Governance Capability

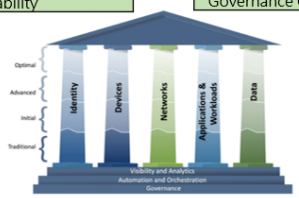
資料來源：CISA、本報告整理

圖6　CISA 新舊版本差異(識別功能面向)

其他差異部分如在設備(Devices)面向之資產管理功能增加考量供應鏈風險與設備威脅防護，在網路(Network)面向新增考量網路流量管理與網路韌性兩個功能。供應鏈風險以組織風險角度，建立供應鏈管理機制，確認可接受之風險與韌性要求；就設備威脅防護則為部署與整合設備威脅防護機制，且要求應有一致性之安全基準。網路流量管理著重於藉由實施動靜態網路規則與組態，管理與監控網路流量。而網路韌性則希望配過良好之網路配置與組態設定，達到每階段成熟度要求之韌性程度，差異處詳見圖 7。

CISA Zero Trust Maturity Model 1.0 Device Pillar	CISA Zero Trust Maturity Model 2.0 Device Pillar
Compliance Monitoring	Policy Enforcement & Compliance Monitoring
Asset Management	Asset & Supply Chain Risk Management
Data Access	Resource Access (Formerly Data Access)
	Threat Protection
Visibility and Analytics Capability	Visibility and Analytics Capability
Automation and Orchestration Capability	Automation and Orchestration Capability
Governance Capability	Governance Capability

CISA Zero Trust Maturity Model 1.0 Network/Environment Pillar	CISA Zero Trust Maturity Model 2.0 Networks Pillar
Network Segmentation	Network Segmentation
Threat Protection	
	Network Traffic Management
Encryption	Traffic Encryption (formerly encryption)
	Network Resilience
Visibility and Analytics Capability	Visibility and Analytics Capability
Automation and Orchestration Capability	Automation and Orchestration Capability
Governance Capability	Governance Capability



資料來源：CISA、本報告整理

圖7　CISA 新舊版本差異(設備/網路功能面向)

在應用程式與工作負載(Applications and Workloads)面向之新增考量安全軟體發展與安全部署，要求應有專案管理系統開發、設計及部署等流程，包含開發、測試、維運環境等之管理與變更流程。在資料(Data)面向新增考量資料分類與資料可用性兩個功能，則要求具體進行資料分類，並定期審查。可用性則可透過備份、備援及動態優化處理，達成資料可用性，差異處詳見圖 8。

CISA Zero Trust Maturity Model 1.0 Application Workload Pillar	CISA Zero Trust Maturity Model 2.0 Applications and Workloads Pillar
Access Authorization	Application Access (formerly access authorization)
Threat Protections	Application Threat Protections (formerly Threat Protections)
Accessibility	Accessible Applications (formerly Accessibility)
Application Security	Application Security Testing (formerly Application security)
	Secure Application Development and Deployment Workflow
Visibility and Analytics Capability	Visibility and Analytics Capability
Automation and Orchestration Capability	Automation and Orchestration Capability
Governance Capability	Governance Capability

CISA Zero Trust Maturity Model 1.0 Data Pillar	CISA Zero Trust Maturity Model 2.0 Data Pillar
Inventory Management	Data Inventory Management
Access Determination	Data Access
Encryption	Data Encryption
	Data Categorization
	Data Availability
Visibility and Analytics Capability	Visibility and Analytics Capability
Automation and Orchestration Capability	Automation and Orchestration Capability
Governance Capability	Governance Capability

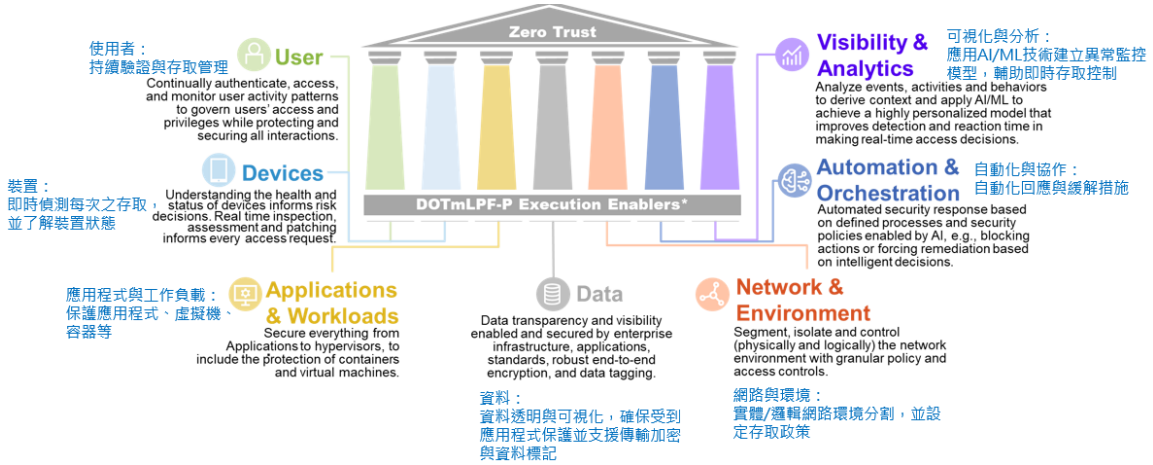
資料來源：CISA、本報告整理

圖8　CISA 新舊版本差異(應用程式與工作負載/資料功能面向)

最後說明成熟度模型的導入與評估階段從所分類之 4 個階段，每一階段皆有其對應之技術要求領域。以成熟度「最佳化」之每個能力支柱為範例，如「識別」要求有持續驗證與風險分析與組織整體識別之一體性；「設備」要求有持續實體與虛擬資產分析，應包含供應鏈管理與整合之威脅防範等；「網路」要求具備分散式微邊界，具有即時且足夠之存取控制與防護韌性；「應用程式與工作負載」要求透過公共網路提供之應用程式應持續要求授權，針對所有工作負載應提供對抗複雜多樣攻擊之防範措施；「資料」要求持續資料盤點與動態存取控制等。

第二個研究方向為美國國防部(Department of Defense, DoD)之零信任策略，以專案計畫推動導入零信任架構，其推動目標設定 116 年前全部門需導入零信任架構，最終目的為防止攻擊者在網路中橫向移動，竊取或改變資料。計畫中採用 3 種行動方案(Course of Action, CoA)，分別為 CoA 1 零信任基準線、CoA 2 商有雲及 CoA 3 私有雲，主軸則為 CoA 1 零信任基準線，要求設定建立零信任的基準線，以現有的基礎設施與環境來開發，後續 DoD 並訂定不同執行藍圖，規劃實作之達成期程。

DoD 的零信任能力包含七個面向，分別為使用者、設備、應用程式與工作負載、資料、網路與環境、自動化與協作及可視化與分析，每個面向訂定細部之能力要求，詳見圖 9。



資料來源：DoD、本報告整理

圖9　零信任策略之能力要求

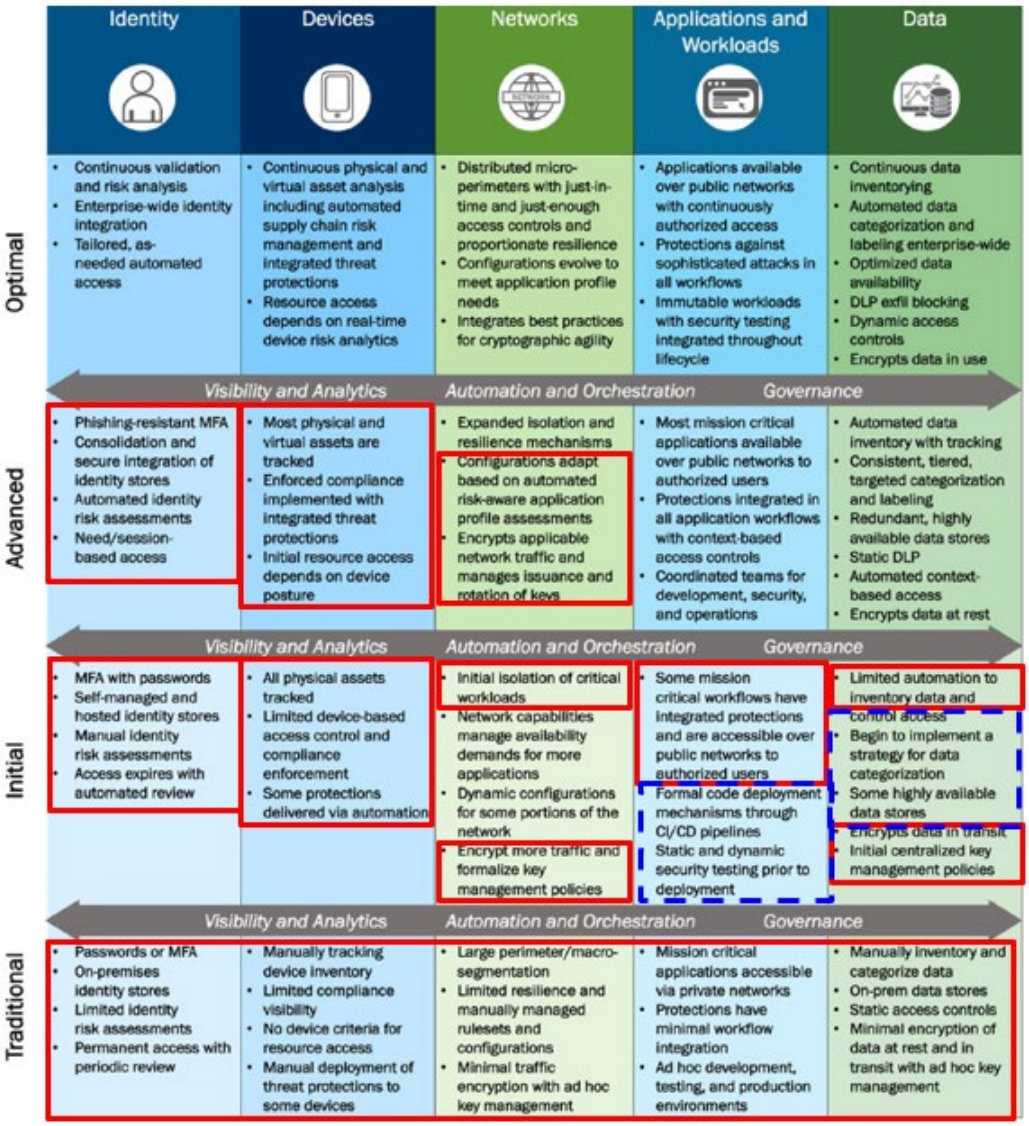
由其策略與藍圖可得知，依零信任七項能力柱，不同能力柱之細項要求，共有 45 個能力(Capabilities)要求，詳見圖 11，其中持續監控與自動化、人工智慧及自動動態政策這 3 個能力歸類為進階等級(Advanced level)，最終所有計畫需於 116 年完成部署零信任架構設定之目標值。

2.2 政府零信任架構推動發展與建議

現行政府零信任架構推動發展主要依據「國家資通安全發展方案(110 年至 113 年)」之推動策略，發展零信任架構資安防護環境，推動政府機關導入零信任架構。整體架構參考國際間之零信任標準、原則及指引，同時參酌我國國情規劃政府零信任架構之推動與發展。導入過程並結合向上集中之防護需求，採取資源門戶之部署方式(Resource Portal-Based Deployment)，以身分鑑別、設備鑑別及信任推斷為 3 大核心機制，身分鑑別為例採用多因子身分鑑別與身分鑑別聲明，設備鑑別主軸則包含設備鑑別與設備健康管理，以及使用者情境進行信任推斷。

首先就我國政府零信任架構與 CISA 發布零信任架構成熟度模型 2.0 比較，目前我國政府零信任架構在「身分」、「設備」及「網路」等 3 個面

向已具備成熟度進階階段(Advanced)之大部分能力。而在「應用程式與工作負載」與「資料」等 2 個面向則滿足成熟度起始階段之大部分能力。至於部分成熟度能力尚無法完全對照，如應用程式需先測試再部署與資料分類分級等項目，則可由我國資通安全管理法等相關要求補足其管理能力之成熟度，詳見圖 10，我國政府零信任架構所包含之能力標記為實體框，若管理面制度與法規所包含之能力，標記為虛線框。

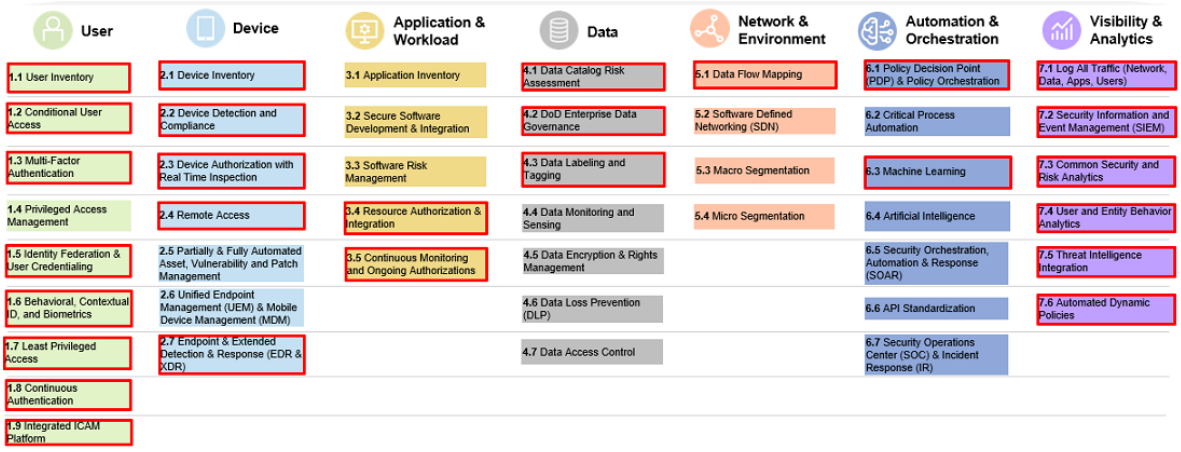


資料來源：CISA、本報告整理

圖10 我國與 CISA 零信任架構成熟度模型比較

CISA 提出的零信任架構成熟度模型可幫助各機關制定零信任策略與實施計畫，依組織安全性與資源配置分階段導入零信任架構，達到不同成熟度等級，亦可避免一次性大規模地替換基礎架構、存取流程及使用者等慣性存取原則，造成負面衝擊及影響，我國零信任架構同樣規劃以階段性方式導入，雖未規劃以成熟度機制為評估主軸，但以身分、裝置及網路等 3 個面向訂定不同檢核與信任等級，與成熟度評估等級有異曲同工之效益，未來亦可評估依資安責任等級要求機關所需達到之零信任成熟度。

第二部分，將 DoD 之零信任策略與我國政府零信任架構對照，現階段我國零信任架構發展規劃已涵蓋 6 成(27/45)美國 DoD 零信任能力，我國政府零信任架構所包含之能力標記紅色框，詳見圖 11。



資料來源：DoD、本報告整理

圖11 零信任策略之能力要求

政府零信任架構針對應用程式與資料本身的安全性，同樣訂有資通安全管理法等相關法規要求保護其安全性，至於對照 DoD 自動化與協調(Automation and Orchestration)部分尚未規劃於我國零信任架構，將在未來期程中逐步擴增零信任架構之整合與完備度，並納入自動化與 AI 新興技術應用之結合能力。

對於政府零信任架構推動發展與建議需關注的另一個重點為美國總務署

(General Services Administration, GSA) 於 112 年所發布零信任架構採購指南，GSA 為美國政府機關之業務經理人及採購代理人，另使用 GSA Schedule 為該機構採購作業制度，凡是通過審核的廠商即可將公司產品或服務置於 GSA Schedule 網站目錄，形式類似我國共同供應契約。目前於 GSA 官網發布零信任架構採購指南是將現有產品與服務，歸類到零信任架構採購之 8 個面向，分別為用戶、設備、網路、基礎設施、應用、資料、可視化與分析及協作與自動化，提供機構採購時參考。因此可發現 GSA 之零信任架構採購指南，並未針對零信任網路解決方案進行整合功能性驗證，機關必須自己依照所公布之採購指南依所需之功能面向採購產品或服務，再自行規劃採購項目之整合。

我國現行作法為於國家資通安全研究院網站設置零信任架構專區，提供通過功能符合性驗證廠商清單，供政府機關具身分鑑別、設備鑑別及信任推斷之完整零信任架構系統清單時參考。而所有通過驗證之廠商，則需參考網站之政府零信任架構說明，確認其產品與服務之功能符合性，再經由資安院團隊進行產品功能符合性實機驗證流程，確認功能實際符合檢查表項目後，即登載於官網上。而網站上所提供之文件目的則希望協助政府機關與業界廠商了解零信任架構之推動政策、相關技術、導入方式及產品需求。

未來將持續發展零信任產品整合性驗證，並鼓勵政府機關採構通過驗證之整合性零信任產品。後續持續參考全球資安標準與技術發展趨勢，如 FIDO(Fast Identity Online)聯盟標準、CC(Common Criteria)標準、PQC(Post Quantum Cryptography)後量子加密標準、關注與零信任相關之新興資安技術，俾針對我國零信任之發展提出相關精進與發展之規劃藍圖。

3.資安技術研析_微軟支援診斷工具 Follina 漏洞分析與驗證實作

本季探討之資安技術研析為微軟支援診斷工具 Follina 漏洞分析，此漏洞於 111 年被揭露，對應美國非營利組織 MITRE 之漏洞編號為 CVE-2022-30190。雖業者於漏洞被發現後已公告修補程式，惟本(112)年於全球攻擊行動中，發現駭客利用業者系統上已知之不同漏洞串聯攻擊流程後，成功入侵受害者電腦並植入木馬程式 LokiBot，此惡意程式允許駭客能遠端存取受駭者之 Windows 系統，從中蒐集憑證與機敏資訊，為熱門之資訊竊取惡意軟體。

Follina 漏洞為網路安全研究團隊@nao_sec，於去年分析一份來自白俄羅斯提交至 VirusTotal 之惡意 Word 文件，該文件可利用微軟支援診斷工具(Microsoft Support Diagnostic Tool, MSDT)之零時差漏洞進行 PowerShell 注入攻擊，且 CVSS 評分為 7.8 分，屬高風險漏洞。由於微軟因未能立即提供解決方式，最初僅發出公告呼籲使用者停用相關通訊協定，以緩解相關風險。而當時 Follina 漏洞於發布安全性更新前即已遭駭客利用，研究人員分析結果顯示，即使關閉巨集仍可觸發該漏洞。駭客便利用此種可透過遠端程式碼執行之漏洞，將內含惡意程式之附件，以網路釣魚方式寄送予鎖定之目標對象進行攻擊。

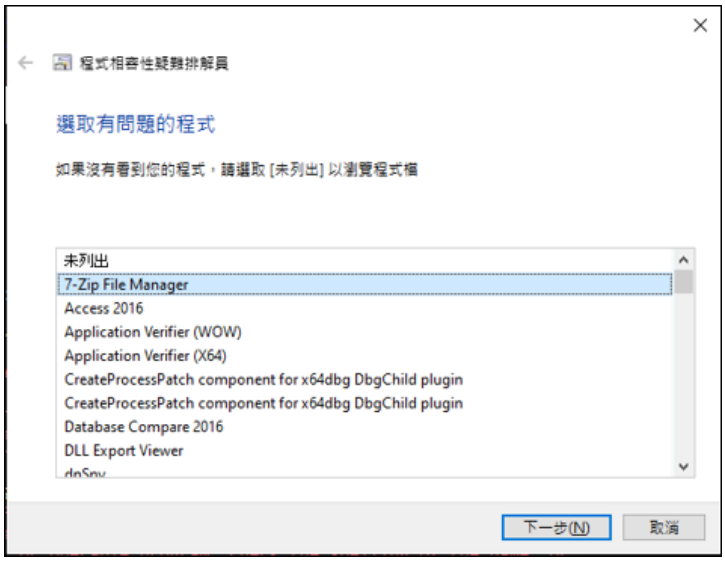
由上述漏洞發展歷程可知，若業者未能即時提供漏洞修補程式，再加上管理者或使用者疏於組態管理之設定，則可能暴露於高風險情境中。以下將概述此漏洞成因、驗證實作攻擊流程及修補說明。

3.1 Follina 漏洞概述與成因

Follina 漏洞存在於微軟支援診斷工具(Microsoft Support Diagnostic Tool, MSDT)中，此工具為 Windows 故障排除平台(Windows Troubleshooting Platform, WTP)主程式，主要用於提供自動化檢測與修復方式，程式名稱

為 msdt.exe。WTP 框架提供使用者或應用程式啟動對應之故障排除程序，依據不同之問題情境，可啟動不同之疑難排解員程式，如程式停止運作、網路連線異常及沒有聲音等情境皆有對應之疑難排解員程式，而每種疑難排解員皆需透過 msdt.exe 執行。

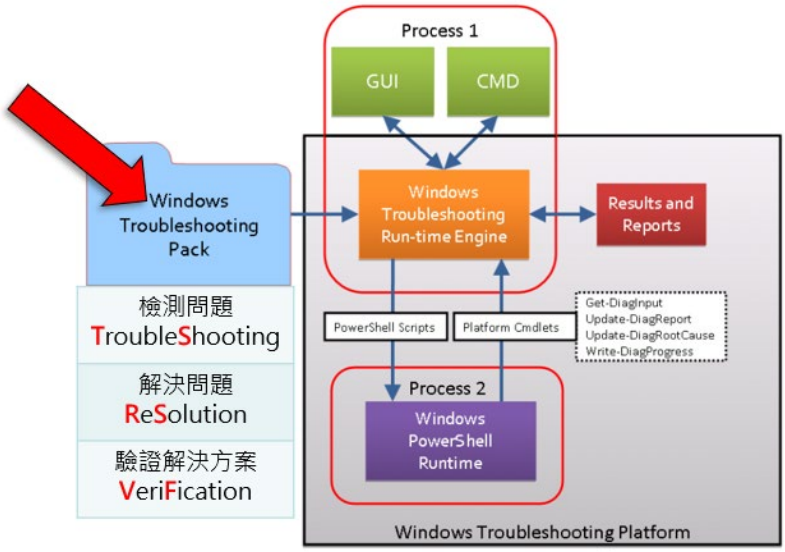
Windows 作業系統亦可透過 ms-msdt 協定啟動疑難排解員程式，此種協定類似 Http 協定，可經由瀏覽器(如 Microsoft Edge 與 Google Chrome)開啟。以「程式相容性疑難排解員」為例，若遇到程式無法正常執行時，如開啟舊版程式導致無法正常執行，可透過程式相容性疑難排解員之下拉式選單或瀏覽方式，選擇有問題之程式再加以排除或修復，詳見圖 12。



資料來源：本報告整理

圖12 程式相容性疑難排解員

疑難排解員檢測過程可分為檢測問題、解決問題及驗證解決方案等 3 個階段。由於不同疑難排解員皆有對應之故障排除包(Windows Troubleshooting Pack)，因此故障排除包亦有檢測問題、解決問題、驗證解決方案等 3 個檢測階段，分別對應 TS_、RS_及 VF_等 3 種 PowerShell 腳本，詳見圖 13。



資料來源：本報告整理

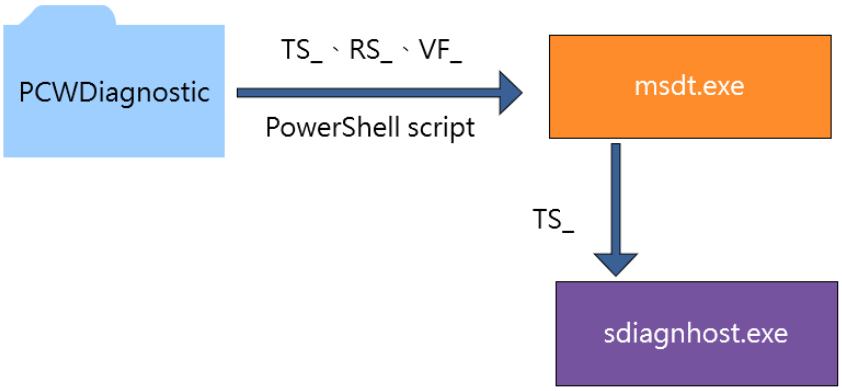
圖13 故障排除包對應之方案

MSDT 工具可透過圖形化介面或命令列 2 種方式執行指令，第一階段 msdt.exe(如圖 13 之 Process 1)，接收 PowerShell 故障排除包腳本後，則會依序傳遞予 Process 2 執行。第二階段 sdiagnhost.exe(如圖 13 之 Process 2)，具 PowerShell 執行環境，可執行由 msdt.exe 提供之腳本，透過 Cmdlets 之 4 個功能與 msdt.exe 進行資料交換，如透過 Get-Diaginput 取得使用者於 msdt.exe 輸入之內容。

此次 Follina 漏洞，主因即為「程式相容性疑難排解員」之瀏覽檔案欄位存在 PowerShell 注入漏洞，攻擊者除可輕易於輸入程式檔處注入 PowerShell 指令外，亦可透過 ms-msdt 協定觸發執行指令。

接下來以執行 Windows 作業系統之小算盤為例進行說明。首先執行指令：msdt.exe ms-msdt:/id PCWDiagnostic /skip force /param “IT_RebrowseForFile=? IT_LaunchMethod=ContextMenu IT_BrowseForFile=/../../$(calc)/.exe”。msdt.exe 依據 id 參數取得 PCWDiagnostic 故障排除包，msdt.exe 再將第 1 階段 TS_腳本(檢測問題)傳

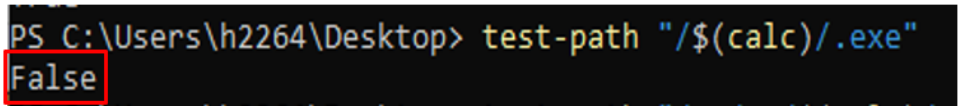
遞予 sdiagnhost.exe 執行，詳見圖 14。



資料來源：本報告整理

圖14 TS_腳本傳遞至 sdiagnhost.exe

下一步驟 sdiagnhost.exe 透過 RunScript 函式之 AddScript 函式新增 TS_腳本，再由 ExecuteCommand 函式執行該腳本，透過 text 變數得知 TS_腳本完整路徑與名稱，腳本名稱為 TS_ProgramCompatibilityWizard.ps1。TS_腳本透過 Get-DiagInput 方法取得 msdt.exe 參數資料，包含 IT_BrowseForFile。TS_腳本將檢查 IT_BrowseForFile 是否為合法路徑，首先，使用 test-path 檢測路徑是否存在，並回傳 True 或 False，詳見圖 15。

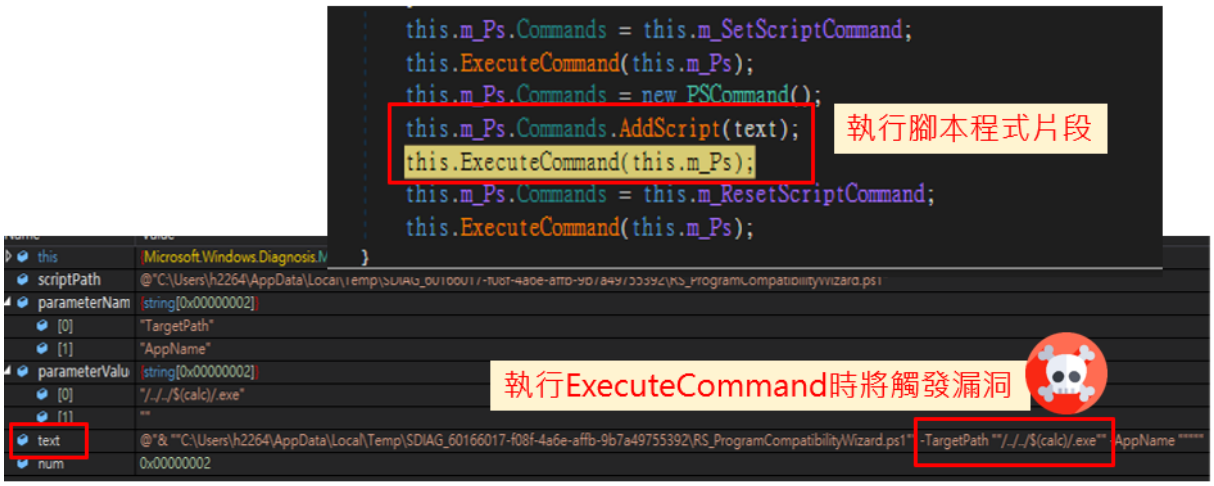


資料來源：本報告整理

圖15 合法路徑確認

而若透過增加多個「../」切換路徑於根目錄之前，則會回傳 True；之後透過檢查副檔名是否為.exe 或.msi 以確認路徑合法性。通過合法路徑檢查後，會將路徑中檔案名稱的「$」字符替換成「`$」的組合，以防止指令被執行。而攻擊指令中 IT_BrowseForFile 之字串「/../../$(calc)/.exe」，滿足上述三個檢查措施，因此 msdt.exe 接續發送 RS_腳本予 sdiagnhost.exe 執

行。sdiagnhost.exe 透過 RunScript 函式執行 RS_腳本，利用將 IT_BrowseForFile 資料放入 text 參數中，使 text 字串帶有「$」字符之惡意指令，執行 ExecuteCommand 函式解析 text 字串時，將觸發漏洞，成功執行系統上之小算盤程式 calc.exe，詳見圖 16。



資料來源：本報告整理

圖16 透過執行指令觸發漏洞

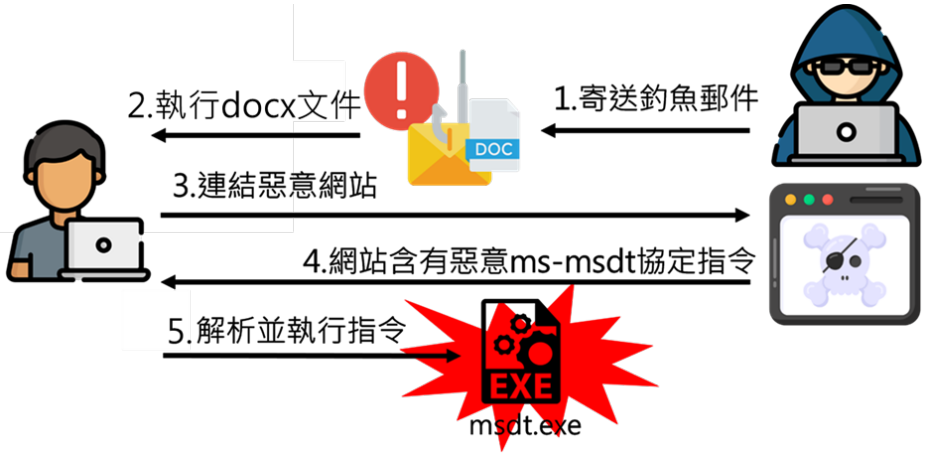
3.2 漏洞攻擊驗證實作與修補

主要驗證流程共分幾個步驟，包含有實作下載概念性驗證(Proof of Concept, PoC)攻擊程式、修改 Exploit.html、架設 Html 網站、修改 docx 與製作 rtf 及執行 docx 與預覽 rtf。首先於 Github 網站下載 PoC 攻擊程式，接續修改 Exploit.html，因文件中之 mhtml 協定會檢查網頁資料是否大於等於 4,096bytes，為符合此限制而插入多行註解，並修改 ms-msdt 協定中之 IT_BrowseForFile 參數，替換為惡意 PowerShell 指令，詳見圖 17。

資料來源：本報告整理

圖17 替換惡意 PowerShell 指令

接續架設 Html 網站，使用 Python3 架設簡易 Http Server，網站存放 Exploit.html 網頁。準備修改 docx 文件與製作 rtf 文件，將 clickme.docx 副檔名調整為壓縮檔「zip」，另需修改 word/_rels/document.xml.rels，將 mhtml 協定中的網址改為所架設之 Http Server 網址，再將副檔名改回 docx，並另存檔案為 rtf 格式。最後開啟 docx 文件後，將自動觸發漏洞執行指令。若為 rtf 文件格式，開啟檔案總管之預覽窗格，並預覽 rtf 文件即可觸發漏洞。依照上述漏洞攻擊驗證實作，則可分為步驟一，使用者下載釣魚郵件中之惡意 docx 或 rtf 格式文件；步驟二，執行 docx 文件，或以預覽模式檢視 rtf 文件；步驟三，文件透過 mhtml 協定，自動連線至帶有 ms-msdt 協定指令之惡意網站；最後透過使用者電腦執行惡意指令，完成遠端執行程式碼攻擊(Remote Code Execution, RCE)，整體攻擊步驟示意圖，詳見圖 18。



資料來源：本報告整理

圖18 攻擊實作步驟

從實作驗證中得知，駭客利用社交工程釣魚郵件，透過惡意 word 文件或 rtf 文件觸發弱點以執行惡意程式。另外，於微軟釋出安全性更新後，比對 Follina 漏洞修補程式內容，發現其於 RunScript 函式新增字串檢查功能，可防範再遭插入惡意指令。然而本年 2 月時微軟以基於安全性考量為由，於官網宣告將於 114 年正式停用支援診斷工具，並將相關功能轉移至取得協助(Get Help)應用程式。

此安全考量或許可由資安廠商 Purplesec 與 Astra Security 之漏洞統計數據看出端倪，此 2 家業者分別於 111 年 12 月與 112 年 4 月發表 111 年前 10 名之常見漏洞，Follina 漏洞排名分別位於第 2 名與第 9 名，表示此漏洞風險仍高，再加上利用 Follina 漏洞攻擊之資安事件迄今仍時有耳聞，建議管理者仍應從風險源頭分析，分析與識別風險後，全面檢視組態安全設定，調整至適切管理狀態，避免遭受相關攻擊

4. 結論

本季具指標性案例為美國 CISA 發出警訊，揭露駭客組織 CyberAv3ngers 正透過 Unitronics 可編程邏輯控制器破壞美國之供水設施，駭客透過 Unitronics PLC 人機介面不良之設定造成，如暴露於公眾網路或弱密碼成功入侵。另一起案例基因檢測提供業者 23andMe 大規模資料外洩，影響數百萬位客戶，業者聲稱是因駭客使用憑證填充攻擊，獲得合法權限存取該平台，又因內部資料檔案未訂定適切之權限存取區隔，造成影響範圍擴大。

國內部分，分析政府資安威脅現況，發現政府機關通報事件原因，以「非法入侵」類型為主，排除綜合類型「其他」外，其次分別為「設備問題」與「網頁攻擊」為主要通報類型。針對本季全球與政府所面臨之主要資安威脅，本報告就「工控系統之資安管理」與「憑證填充攻擊手法之資安管理」提出資安防護建議。

資安專題分享主題為零信任架構近期發展現況說明與推動建議，從美國所發布之零信任架構，如 CISA 零信任成熟度模型、DoD 零信任策略及 GSA 信任架構採購指引，對照我國零信任架構之發展與推動情形，並提出後續零信任持續精進方向。

另外，資安技術研析主題為微軟支援診斷工具之 Follina 漏洞分析，漏洞編號為 CVE-2022-30190，駭客便利用此種可透過遠端程式碼執行之漏洞，將內含惡意程式之附件，以網路釣魚方式寄送予鎖定之目標對象。此漏洞於 111 年被揭露此風險，惟近期又於全球攻擊行動中，發現駭客利用業者系統上已知且不同漏洞串聯攻擊流程後，成功入侵受害者電腦並植入木馬程式 LokiBot，政府機關應加強安全組態、系統更新及提防漏洞組合之攻擊。

資安相關活動

本季數位發展部資通安全署辦理之資安相關活動，說明如下。

◆ 跨國攻防演練 CODE 2023

行政院國家資通安全會報每 2 年辦理 1 次大規模跨國攻防演練(Cyber Offensive and Defensive Exercise, CODE)，112 年辦理日期自 10 月 18 日至 10 月 20 日止，活動目的期藉由攻防演練檢視關鍵基礎設施提供者之通報應變作業與資安防護完備度，並於期間邀請國內外專家參與實際攻防與經驗交流分享。

此次以水資源領域做為模擬演練場域，邀請國內外資安攻擊好手與水資源領域關鍵基礎設施提供者(台灣自來水公司)進行紅藍隊技術攻防，模擬以淨水民生工控設備發現來自組織外部網路駭侵組織入侵，且最終影響水資源之提供。演練防禦方需因應此次攻擊，分析入侵原因與路徑，以辦理通報及應變程序。於攻防演練活動後，安排研討會就紅藍對抗技術攻防結果與各國訪賓進行實務研討。藉由實際演練與研討會，本次演練與參與人員能充分進行經驗分享及共同學習，提升彼此資安攻防技術與應變能力，進而促進跨國聯防與深化國際合作

◆ 112 年第 2 次政府資通安全防護巡迴研討會

第 2 次政府資通安全防護巡迴研討會於 11 月期間辦理，分別於台北、台中、高雄及台東等地共辦理 8 場研討會。政府資通安全防護巡迴研討會主要針對資通安全管理法納管對象之資安專職(責)人員，期許透過研討會方式宣導政府機關資安威脅與防護重點、宣導最新資安防護重點與訊息，協助各機關提升資通安全管理與技術認知，本次議題共有資通安全業務重點工作、政府機關資安威脅與防護重點及 112 年網路攻防演練暨資安檢測重要發現事項。

議題一為資通安全業務重點工作，說明資通安全管理法遵事項現行推動辦理情形、重點工作宣導及近期政府機關資安事件案例分享及防護建議，如機關網頁驗證通行碼編號原則相同，且因使用流水號易遭猜測又未採多因子認證、漏洞未修補遭上傳惡意程式及供應商出現資安管理等議題。議題二為資安威脅趨勢與案例分享，分享全球與資通安全威脅趨勢，對於相關威脅趨勢，規劃資安防護強化重點，從全球全球資通安全威脅趨勢，分析與統計政府資通安全威脅趨勢，再從政府資安事件案例分析，提供防護建議，包含強化偵測防護以因應資安威脅、強化社交工程郵件防範、落實設備定期更新檢視暨執行及落實委外管理降低供應鏈風險。議題三為 112 年網路攻防演練暨資安檢測重要發現事項，包含未落實通行碼強度檢查機制，造成認證及驗證機制失效、注入漏洞、限制存取功能失效，致無效之存取控制及因不安全的組態設定，並未確實限制檔案上傳類型及帳號密碼外洩等，針對相關攻防演練暨資安檢測重要發現事項，亦於報告中提供防護建議。