107年第4季資通安全技術報告

Quarterly Technical Report

目　次

第一章 資安威脅現況與防護重點 1
1.1 全球資安威脅現況 1
1.2 政府資安威脅現況 2
1.3 資安防護重點 5
第二章 資安專題分享 7
2.1 資通系統防護基準要求 7
2.2 資通系統安全控制措施說明 11
第三章 資安新興議題研討 19
3.1 滲透 Air-Gapped Network 之 Ghost Tunnel 攻擊 19
3.2 WebDAV 緩衝區溢位漏洞攻擊 23
第四章 結論 26
資安相關活動 27
資安巡迴宣導 27
資安服務廠商評鑑 27
參考文獻 29

圖 目 次

圖 1　107 年第 4 季資安事件影響等級比率圖 3
圖 2　107 年第 4 季資安事件通報類型比率圖 4
圖 3　107 年第 4 季資安事件原因比率圖 5
圖 4　拒絕存取畫面 12
圖 5　利用 Java Servlet Filter 實作 12
圖 6　利用 ASP.NET URL 授權實作 13
圖 7　觸發特定事件所產生之 Log 13
圖 8　管理者帳號操作系統所產生之 Log 14
圖 9　設定 Log 輸出格式 14
圖 10　指定演算法與協定(protocol) 15
圖 11　Apache Tomcat 設定檔範例 16
圖 12　身分驗證機制 17
圖 13　驗證碼實作範例 17
圖 14　要求重設密碼 18
圖 15　重設密碼連結設定 18
圖 16　Air-Gapped Network 入侵流程 19
圖 17　設備與 WiFi 連接示意 21
圖 18　利用隨身碟或社交工程植入惡意程式 21
圖 19　利用偽冒 AP 誘騙受害者連線 22
圖 20　開啟 Ghost Tunnel Server 進行連線 22
圖 21　透過具 WebDAV 協定之工具遠端管理功能 23
圖 22　駭客利用 Buffer Overflow 漏洞進行攻擊手法 25

表 目 次

表 1　資通系統防護基準 7
表 2　普級資通系統之技術面控制措施 8
表 3　中級資通系統之技術面控制措施 9
表 4　高級資通系統之技術面控制措施 10
表 5　WebDAV 增加的指令 24

摘要

「第 4 季資通安全技術報告」除分析本季全球資安威脅、政府通報之資安事件外，並提供相對應之防護建議。同時，藉由資安專題之分享與資安新興議題之研討，提供政府機關(構)於資安風險的關注重點。

「第 4 季資通安全技術報告」分為以下 4 個章節。

●第 1 章：資安威脅現況與防護重點

從分析全球資安威脅現況開始，第一起案例探討關鍵資訊基礎設施之資安風險，美國政府責任署針對美國國防部的武器系統發表一篇滲透研究報告，指稱美國國防部的主要武器系統缺乏嚴密的安全機制，只要利用簡單的工具及技術，就可在不被察覺的情況下掌控相關系統。

第二起案例為駭客利用供應鏈漏洞入侵事件，駭客先入侵熱門的網路分析平台 StatCounter，在 StatCounter 上植入惡意的 JavaScript，藉以攻擊利用 StatCounter 分析流量的網站，受害者則為加密貨幣交易平台 gate.io。

分析政府資安威脅現況，發現政府機關(構)通報事件原因以網站設計不當(占 26.55%)、其他(占 25%)及弱密碼(占 12.5%)為主。部分機關(構)使用網站管理後台提供管理者上傳檔案功能，因同時存在弱密碼或權限控管不當等原因，遭駭客利用上傳惡意網頁進行網頁置換。

●第 2 章：資安專題分享

資安專題分享說明 107 年 11 月 21 日所公告的「資通安全責任等級分級辦法」之資通系統防護基準要求之重要控制措施，協助機關(構)了解技術面實作項目。同時特別針對技術面部分說明驗證方法與實作範例，協助機關(構)了解技術面安全性設定，以強化系統安全性，並符合法規要求。

●第 3 章：資安新興議題研討

由資安研究人員整理之資安新興議題，包括 2 大主題。

第 1 個議題為滲透 Air-Gapped Network 之 Ghost Tunnel 攻擊，說明 Ghost Tunnel 的功能及攻擊手法。Air-Gapped Network 入侵來源可能來自供應鏈攻擊、受騙的內部使用者或惡意的內部使用者，藉由於網路內任意一台植入惡意程式，操作及連線途徑包括無線電頻率、蠕蟲與病毒等自動擴散手法。

第 2 個資安新興議題則為 WebDAV 緩衝區溢位漏洞攻擊。WebDAV 為 HTTP 延伸的協定，提供遠端維護網站資料服務，使用者可透過具 WebDAV 協定之工具，遠端管理網站/系統文件。CVE-2017-7269 為 WebDAV 服務存在緩衝區溢位弱點，允許攻擊者遠端執行任意程式碼或造成阻斷服務的安全漏洞。

●第 4 章：結論

本報告透過分析全球與政府之資安事件與統計數據，了解最新資安威脅現況與因應之防護重點。同時，因應資通安全管理法施行，資安專題分享資通系統防護基準要求資通系統依其安全等級必須符合之控制措施，亦針對技術面實作加以說明。此外，透過 2 個資安新興議題的研討，深入探討技術主題、駭客攻擊手法及因應方式。在掌握本季之資安威脅現況時，亦說明下一季之資安專題重點，將剖析物聯網設備之漏洞與因應。

第一章 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與可能之衝擊與影響。組織內部一旦存在脆弱點，如弱密碼或系統防護不足等，可能導致駭客輕易入侵到內部，或成功竊取機敏資料等嚴重後果。本章節的事件與議題皆配合整理相關之防護重點，提供組織就相關資安風險或議題討論，並可依循防護重點規劃執行細節。

1.1 全球資安威脅現況

研析全球網路攻擊事件可歸納出 6 大面向之全球資安威脅趨勢，分別為「進階持續威脅攻擊竊取機密資料」、「分散式阻斷服務攻擊癱瘓網路運作」、「物聯網設備資安弱點威脅升高」、「關鍵資訊基礎設施資安風險倍增」、「網路與經濟罪犯影響電子商務與金融運作」及「資安(訊)供應商持續遭駭破壞供應鏈安全」。全球所面臨之資安威脅不僅複雜且具多樣化，即早針對攻擊進行準備，以防患於未然，會是很好的防禦策略，但如何提升本身的資安韌力亦是值得探討的進階議題。

第 4 季(以下簡稱本季)具指標性的案例為關鍵資訊基礎設施因防護機制不足，存在遭滲透之潛在風險；另一起案例為駭客利用供應商入侵加密貨幣交易平台。

首先，探討「關鍵資訊基礎設施資安風險倍增」案例，美國政府武器系統缺乏嚴密的安全機制，美國政府責任署(Government Accountability Office，以下簡稱 GAO)於 107 年本季針對美國國防部(Department of Defense，以下簡稱 DOD)的武器系統發表一篇滲透研究報告，指稱 DOD 的主要武器系統缺乏嚴密的安全機制，只要利用簡單的工具及技術，就能在不被察覺的情況下掌控相關系統。有鑑於 DOD 正打算支出 1.66 兆美元來發展武器系統，潛在的對手則已開發鎖定 DOD 的網路間諜/攻擊技術。GAO 針對 DOD 的各式武器系統展開滲透測試，其中有團隊只花 1 個小時就入侵其

中一個武器系統，接著用 1 天時間取得該武器系統的完整控制權。

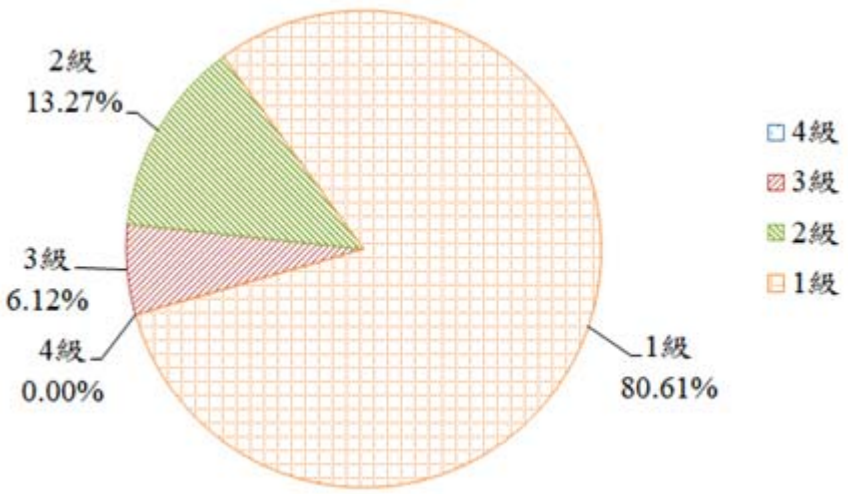
第二起案例為駭客利用供應商入侵加密貨幣交易平台，此案例為遭駭客鎖定之「資安(訊)供應商持續遭駭破壞供應鏈安全」事件。資安業者 ESET 於 107 年 11 月 6 日揭露一起利用供應鏈漏洞入侵事件，駭客先入侵熱門的網路分析平台 StatCounter，在 StatCounter 上植入惡意的 JavaScript，藉以攻擊利用 StatCounter 分析流量的網站，受害者為加密貨幣交易平台 gate.io。各家網站如欲利用 StatCounter 分析網路流量，可在需要追蹤訪客流量的網頁上嵌入 www.statcounter[.]com/counter/counter.js，駭客竄改了此一 JavaScript 檔案注入惡意程式，讓程式先檢查採用該 JavaScript 的網址是否含有通用資源識別碼(Uniform Resource Identifier, URI)「myaccount/withdraw/BTC」。根據 ESET 的報告，由於此為 gate.io 平台特有之 URI，顯示駭客是瞄準比特幣的交易網頁而來。駭客在確定流量來自 myaccount/withdraw/BTC 後，會再注入另一個腳本程式，則可自動將比特幣的轉帳位址改成駭客所掌控的加密貨幣錢包。

綜覽本季重大資安事件，關鍵資訊基礎設施提供之資訊服務，因涉及國家、社會、經濟及民眾等不同層面，不難窺探出駭客為何鎖定關鍵資訊基礎設施持續進行目標式攻擊，資安風險亦應層層挖掘並重視。面對供應鏈可能造成之防禦層面上的漏洞，組織在選擇供應鏈時，須要求一致性之資安防護度，或於合約期間定期檢視供應鏈之資安防護，相關監督管理措施可降低資安風險發生之可能性。

1.2 政府資安威脅現況

彙整本季所接獲之政府機關(構)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(構)之資安威脅現況。通報事件依資安事件對「機密性」、「完整性」、「可用性」3 個面向所造成的衝擊，將事件影響等級由輕至重分為 1 級、2 級、3 級及 4 級資安事件。彙整事件

影響等級，本季以 1 級事件占 80.61%為大宗，2 級事件占 13.27%次之，3 級事件僅占 6.12%，而 4 級資安事件則未發生，相關統計情形詳見圖 1。

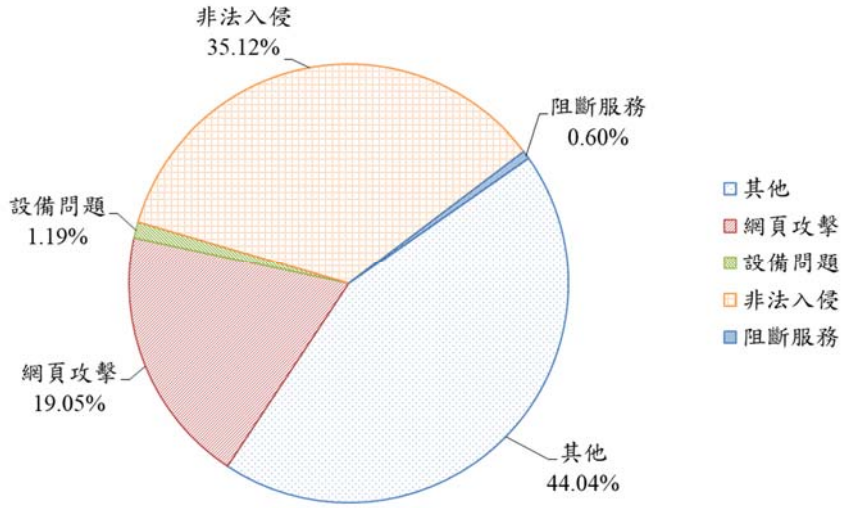


資料來源：本報告整理

圖1　107 年第 4 季資安事件影響等級比率圖

本季 3 級重要資安事件均為攻防演練通報事件，相關弱點包括「機敏資料外洩」、「無效的身分認證」、「注入攻擊」及「無效的存取控管」。

此外，資安事件通報類型依其所發現之異常情形，包括非法入侵、網頁攻擊、設備問題、阻斷服務及其他，其中，又以「其他」(占 44.04%)與「非法入侵」(占 35.12%)等類型為主，詳見圖 2。「其他」類型主要為網路攻防演練遭攻擊成功所通報事件，由於攻防演練事件非屬實際發生之資安事件，故通報類型判定為「其他」。

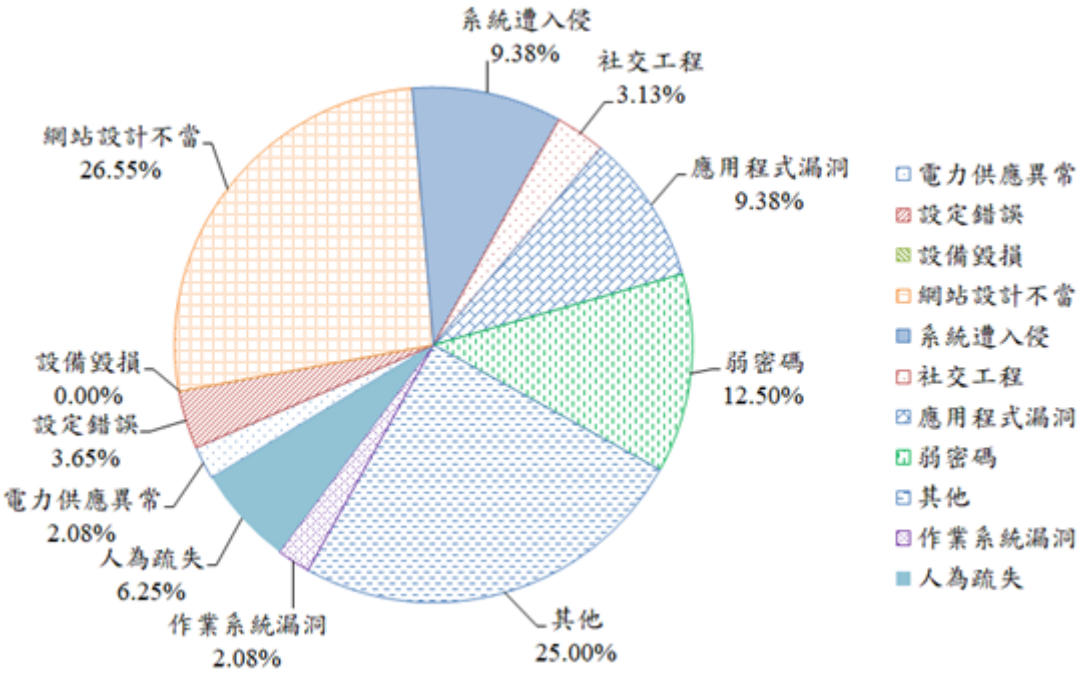


資料來源：本報告整理

圖2　107 年第 4 季資安事件通報類型比率圖

最後，分析通報事件發生原因，以網站設計不當(占 26.55%)為主，其次分別為其他(占 25%)、弱密碼(占 12.5%)、應用程式漏洞 (占 9.38%)、系統遭入侵(占 9.38%)、人為疏失(占 6.25%)、設定錯誤(占 3.65%)、社交工程(占 3.13%)、電力供應異常(占 2.08%)、作業系統漏洞(占 2.08%)及設備毀損(占 0 %)，詳見圖 3。本季事件原因以網站設計不當為主，有 7 成為攻防演練事件通報外，其餘通報案件為一般案件。

再進一步分析事件發生原因，部分機關(構)使用網站管理後台提供管理者上傳檔案功能，因同時存在弱密碼或權限控管不當等原因，遭駭客利用上傳惡意網頁進行網頁置換；另外，部分網站存在本地檔案引入(Local File Inclusion, LFI)漏洞，因網站開發者撰寫 php 時函數使用不當，導致後端系統檔案與網站程式原始碼等敏感資料，遭駭客取得利用而置換網頁。



資料來源：本報告整理

圖3　107 年第 4 季資安事件原因比率圖

1.3 資安防護重點

分析本季全球資安威脅現況，關鍵資訊基礎設施的資安風險持續升溫，促使駭客趨之若鶩的主因，在於成功入侵這些關鍵資訊基礎設施後，所潛藏的包括政治、經濟及其他種種利益都是不容小覷的，且對國家、社會秩序或民眾的影響更是驚人；另外，利用供應鏈漏洞入侵事件是另一個值得關注的重點，類似供應鏈或委外廠商的弱點所引發的資安事件，在業務持續營運夥伴角度上，如何提升供應鏈或委外廠商的資安防護，亦是後續資安強化重點。

分析政府機關(構)通報的資安事件可看出，網站設計不當的事件占比，第 4 季的 26.55%比第 3 季的 24.34%略為升高，顯示網站系統仍被駭客視為主要的攻擊目標。隨著資通安全管理法(以下簡稱資安法)的正式施行，政府機關應依「資通安全責任等級分級辦法」，落實執行資通系統所對應等

級之控制措施，並依循安全系統發展生命週期(SSDLC)進行系統開發與維運，以降低網站設計不當所造成的風險。有關「資通安全責任等級分級辦法」之各等級防護基準要求與控制措施，可參考本報告第 2 章內容。

綜整以上資安威脅現況，提供資安防護建議如下：

●關鍵資訊基礎設施安全之防護

– 分析與評鑑關鍵資訊基礎設施之資安風險，檢視相關脆弱與威脅點。

– 分析類似關鍵資訊基礎設施曾發生之資安事件，並進行事件因應與強化。

– 定期進行關鍵資訊基礎設施網路攻防演練，即時辨識系統弱點。

●身分認證與存取管控安全

– 加強資通系統身分認證與存取機制，以最小權限為開放原則。

– 定期檢視權限開放之必要性與活動日誌，並刪除閒置帳號。

– 嚴格控管委外廠商之連線與開放，連線開放前應先進行風險評估。

●網站設計不當與弱密碼

– 系統上線前，務必進行源碼檢測與弱點掃描。

– 若系統委外開發，則應檢視委外廠商資通系統開發流程是否規劃安全機制。

– 提供資安教育訓練，宣導弱密碼之風險，並輔以系統工具強制使用強度較高之密碼。

第二章 資安專題分享

資安法於 107 年 5 月 11 日立法院三讀通過，107 年 6 月 6 日由總統公告，立法目的在加速建構國家資通安全環境，以保障國家安全，維護社會公共利益。依據資安法之「資通安全責任等級分級辦法」，明定各機關應辦理之資通安全責任等級應辦事項。

本報告說明於 107 年 11 月 21 日公告的「資通安全責任等級分級辦法」，規定資通系統必須符合普、中及高對應等級之控制措施。同時特別針對技術面部分說明驗證方法與實作範例，協助機關了解技術面安全性設定，以強化系統安全性，並符合法規要求。

2.1 資通系統防護基準要求

資通系統防護基準包括存取控制、稽核與可歸責性、營運持續計畫、識別與鑑別、系統與服務獲得、系統與通訊保護及系統與資訊完整性等 7 個構面，共 29 項控制措施，詳見表 1。

表1　資通系統防護基準

構面	數量	控制措施類別
存取控制	3 項	帳號管理/最小權限/遠端存取
稽核與可歸責性	6 項	稽核事件/稽核紀錄內容/稽核儲存容量/稽核處理失效之回應/時戳及校時/稽核資訊之保護
營運持續計畫	2 項	系統備份/系統備援
識別與鑑別	5 項	內部使用者之識別與鑑別/身分驗證管理/鑑別資訊回饋/加密模組鑑別/非內部使用者之識別與鑑別
系統與服務獲得	8 項	系統發展生命週期需求階段/系統發展生命週期設計階段/系統發展生命週期開發階段/系統發展生命週期測試階段/系統發展生命週期部署與維

構面	數量	控制措施類別
		運階段/系統發展生命週期委外階段/獲得程序/系統文件
系統與通訊保護	2 項	傳輸之機密性與完整性/資料儲存之安全
系統與資訊完整性	3 項	漏洞修復/資通系統監控/軟體及資訊完整性

資料來源：資通安全責任等級分級辦法[1]

以技術角度而言，分別針對上述 7 個構面之控制措施類別，就適用於普、中及高級資通系統之控制措施進行說明。

●普級資通系統之技術面控制措施，詳見表 2。

表2　普級資通系統之技術面控制措施

項次	控制措施內容	類別
1	對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化，使用者權限檢查作業應於伺服器端完成	遠端存取
2	確保資通系統有稽核特定事件之功能，並決定應稽核之特定資通系統事件	稽核事件
3	應稽核資通系統管理者帳號所執行之各項功能	稽核事件
4	資通系統產生之稽核紀錄應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，並採用單一日誌紀錄機制，確保輸出格式之一致性	稽核紀錄內容
5	資通系統於稽核處理失效時，應採取適當之行動	稽核處理失效之回應
6	使用預設密碼登入系統時，應於登入後要求立即	身分驗證管理

項次	控制措施內容	類別
	變更	
7	身分驗證相關資訊不以明文傳輸	
8	具備帳戶鎖定機制，帳號登入進行身分驗證失敗達 3 次後，至少 15 分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制	
9	基於密碼之鑑別資通系統應強制最低密碼複雜度；強制密碼最短及最長之效期限制	
10	使用者更換密碼時，至少不可以與前 3 次使用過之密碼相同	
11	資通系統應遮蔽鑑別過程中之資訊	鑑別資訊回饋
12	應注意避免軟體常見漏洞及實作必要控制措施	系統發展生命週期開發階段
13	發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息	

資料來源：本報告整理

- 中級資通系統除完成普級之技術面控制措施外，亦包括以下之控制措施，詳見表 3。

表3　中級(除完成普級外)資通系統之技術面控制措施

項次	控制措施內容	類別
1	已逾期之臨時或緊急帳號應刪除或禁用	帳號管理
2	資通系統閒置帳號應禁用	
3	資通系統應採用加密機制	遠端存取
4	資通系統產生之稽核紀錄，應依需求納入其他相關資訊	稽核紀錄內容

項次	控制措施內容	類別
5	應運用雜湊或其他適當方式之完整性確保機制	稽核資訊之保護
6	身分驗證機制應防範自動化程式之登入或密碼更換嘗試	身分驗證管理
7	密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記	
8	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存	加密模組鑑別
9	使用者輸入資料合法性檢查應置放於應用系統伺服器端	軟體及資訊完整性

資料來源：本報告整理

- 高級資通系統除完成普級及中級之技術面控制措施外，亦包括以下之控制措施，詳見表 4。

表4　高級(除完成普級及中級外)資通系統之技術面控制措施

項次	控制措施內容	類別
1	逾越機關所定預期閒置時間或可使用期限時，系統應自動將使用者登出	帳號管理
2	機關規定需要即時通報之稽核失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告	稽核處理失效之回應
3	定期備份稽核紀錄至與原稽核系統不同之實體系統	稽核資訊之保護
4	對帳號之網路或本機存取採取多重認證技術	內部使用者之識別與鑑別
5	具備系統嚴重錯誤之通知機制	系統發展生命

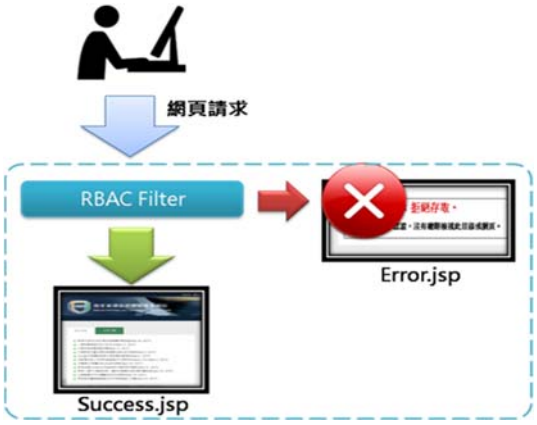
項次	控制措施內容	類別
		週期開發階段
6	資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限	傳輸之機密性與完整性
7	使用公開、國際機構驗證且未遭破解之演算法	
8	支援演算法最大長度金鑰	
9	靜置資訊及相關具保護需求之機密資訊應加密儲存	資料儲存之安全

資料來源：本報告整理

2.2 資通系統安全控制措施說明

前述章節已概述不同構面之控制措施項目相關要求，接續將就相關重要技術面項目說明驗證手法與實作範例。

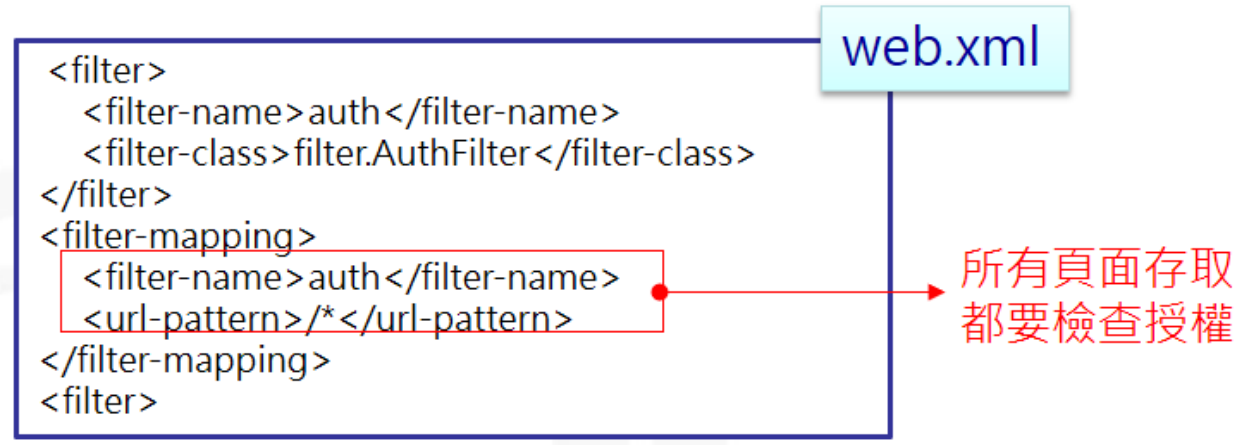
- 遠端存取(普級)：系統應包含具有一致全面性、位於伺服器端、強制適用於全系統的授權及存取控制機制(如使用 Filter 過濾器等)，避免被攻擊者繞過檢查機制。
  - 驗證方法：以測試案例驗證，如停用瀏覽器 JavaScript 功能後，以一般使用者帳號登入，試圖存取他人或管理者頁面之功能，系統應拒絕存取，詳見圖 4。



資料來源：本報告整理

圖4　拒絕存取畫面

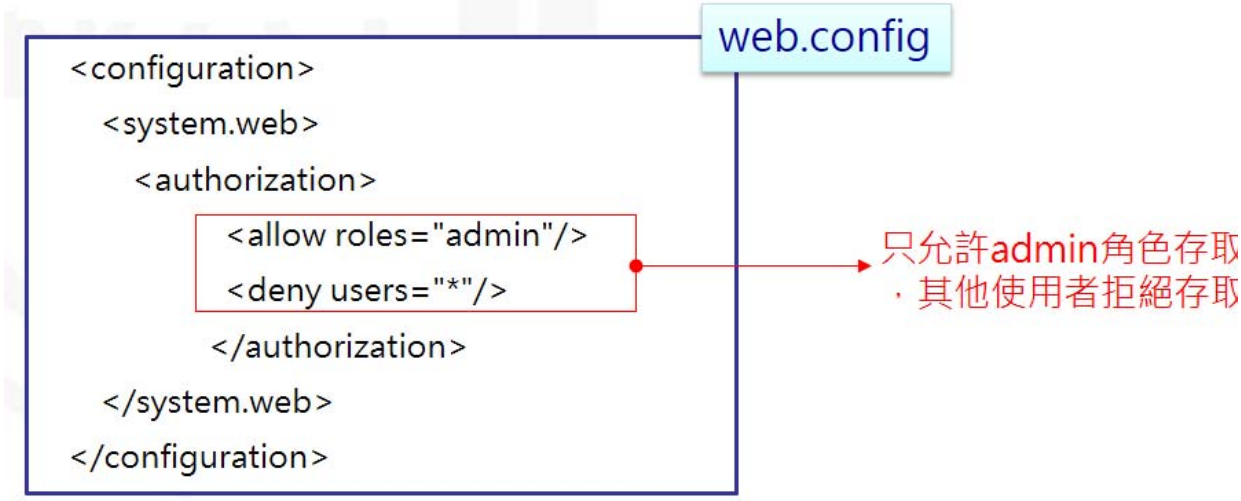
– 利用 Java Servlet Filter 之實作範例，詳見圖 5。



資料來源：本報告整理

圖5　利用 Java Servlet Filter 實作

– 利用 ASP.NET URL 授權之實作範例，詳見圖 6。



資料來源：本報告整理

圖6　利用 ASP.NET URL 授權實作

●稽核事件(普級)：系統留存日誌紀錄之目的如程式除錯、行為歸責、稽核取證及法規要求等；稽核事件如身分驗證失敗、存取資源失敗、重要行為、重要資料異動及功能錯誤等。

– 驗證方法：藉由觸發特定事件以產生相關 Log 紀錄，詳見圖 7。

資料來源：本報告整理

圖7　觸發特定事件所產生之 Log

●稽核系統管理者行為(普級)：稽核管理者行為將有助於定期稽核系統行為及資安事件追查。

– 驗證方法：使用管理者帳號操作系統以產生相關 Log 紀錄，詳見圖 8。

資料來源：本報告整理

圖8　管理者帳號操作系統所產生之 Log

●稽核紀錄內容(普級)：ID 紀錄不可為個資類型(如身分證號等)，同時若採用單一的 Log 機制有助於資安事件追蹤。

– 驗證方法：檢視特定事件或管理者行為之 Log 紀錄，應包含關鍵資訊，並具備一致格式，詳見圖 9。

```
<PatternLayout>
  <Pattern>%d %p %c{1.} [%t] %m%n</Pattern>
</PatternLayout>
```

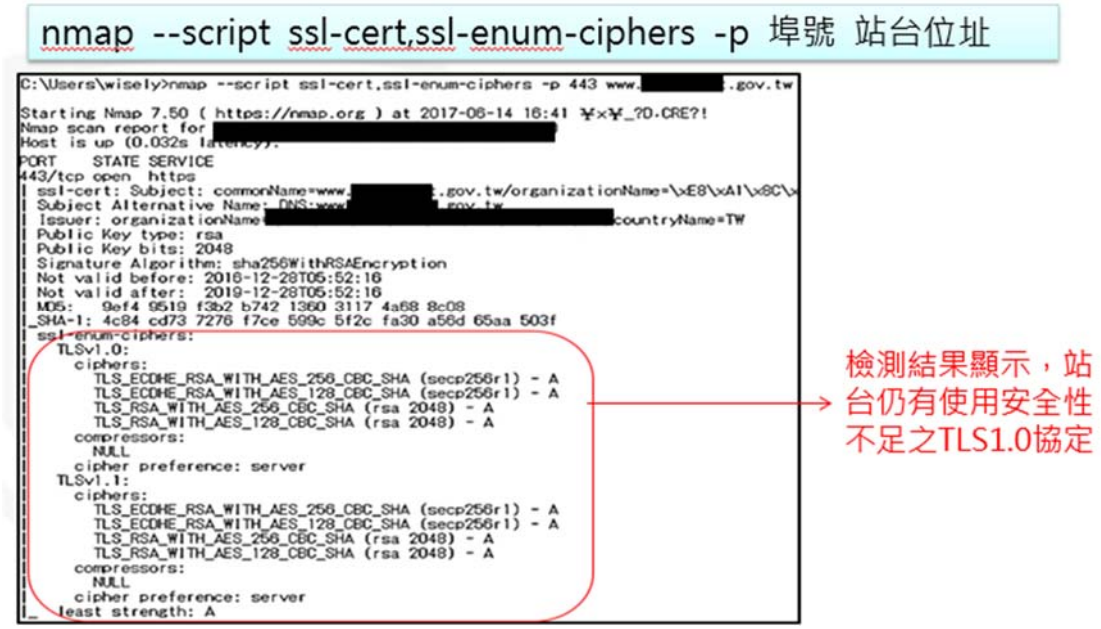
參數	說明
%d	日期時間，可在{}內設定日期格式，日期格式可參考Java的SimpleDateFormat
%c	完整類別名稱，如com.abc.ClassTest
%L	輸出來源於程式碼中的行數
%m	輸出訊息，程式中自訂的訊息
%n	輸出換行符號標記，替輸出紀錄換行
%p	輸出Log等級，如ERROR、DEBUG等
%t	輸出Log所屬執行序名稱

資料來源：本報告整理

圖9　設定 Log 輸出格式

●傳輸加密(普級、高級)：普級基本要求是採用加密傳輸，避免身分驗證資訊被攔截或監聽竊取。避免採用不安全的協定，如 SSL 及 TLS1.0 版本等；避免採用已被破解的演算法，如 RC4、DES 及 3DES 等。若能確定是使用公開、國際機構驗證且未遭破解之演算法或支援演算法最大長度金鑰，則可達到防護需求等級高之要求。

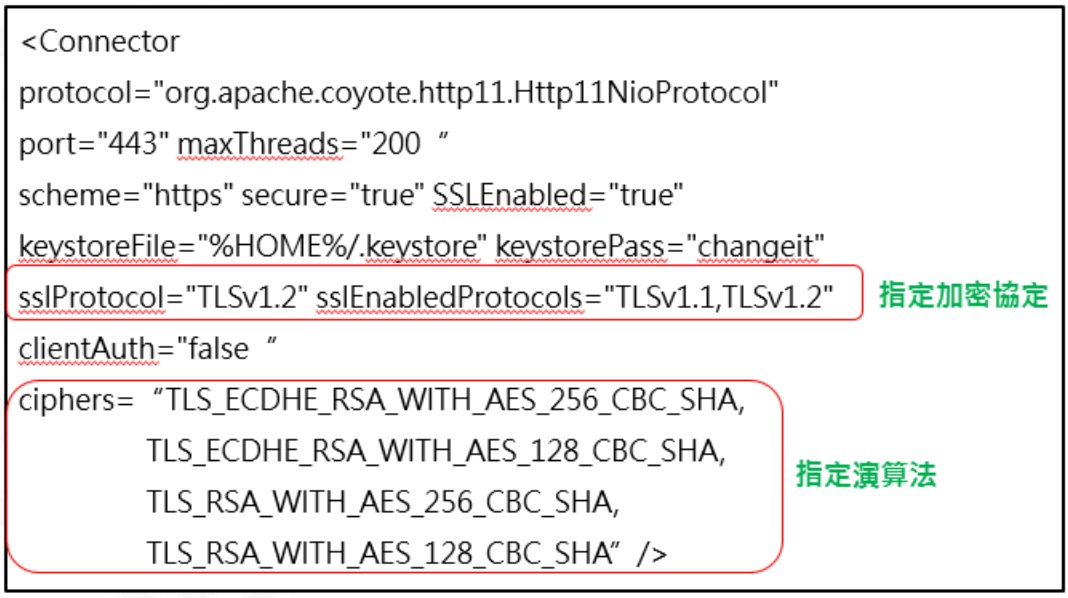
– 驗證方法：可使用 nmap 工具，測試站台所啟用的加密傳輸協定及加密演算法，詳見圖 10。



資料來源：本報告整理

圖10 指定演算法與協定(protocol)

– 實作範例為調整伺服器設定檔，指定傳輸加密協定及演算法，以 Apache Tomcat 設定檔範例，詳見圖 11。



資料來源：本報告整理

圖11 Apache Tomcat 設定檔範例

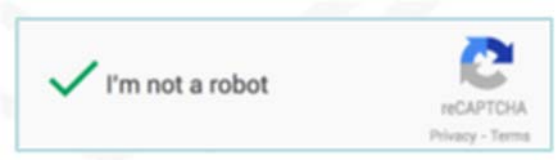
●防自動化程式機制(中級)：身分驗證機制應防範自動化程式之登入或密碼更換嘗試。自動區分電腦與人類的圖靈測試(Completely Automated Public Turing test to tell Computers and Humans Apart, CAPTCHA，俗稱驗證碼)，常用於身分驗證或重要交易行為。

– 驗證方法：輸入錯誤或空白驗證碼，系統應拒絕登入，詳見圖 12。

資料來源：本報告整理

圖12 身分驗證機制

– 使用 Google reCaptcha 之實作範例，詳見圖 13。

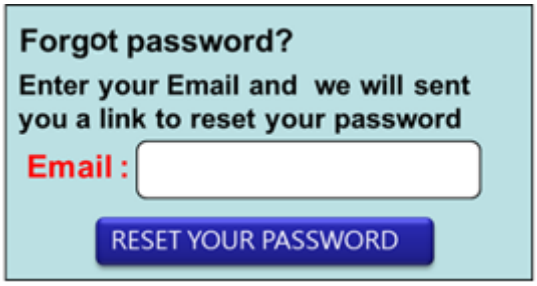


資料來源：本報告整理

圖13 驗證碼實作範例

- 密碼重設機制(中級)：密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。常見作法為先要求使用者輸入 Email 資料並驗證正確性，如系統產生具有時效性之 URL 連結，並發送至該信箱，使用者登入信箱且點選該 URL 連結後，即可使用重設密碼功能頁面。

  – 驗證方法：點選忘記密碼，檢視是否收到 Email，並於時效內進行密碼重設，詳見圖 14。



資料來源：本報告整理

圖14 要求重設密碼

– 驗證實作為確認帳號存在，則將密碼重設功能之連結寄送至原留存信箱，詳見圖 15。

資料來源：本報告整理

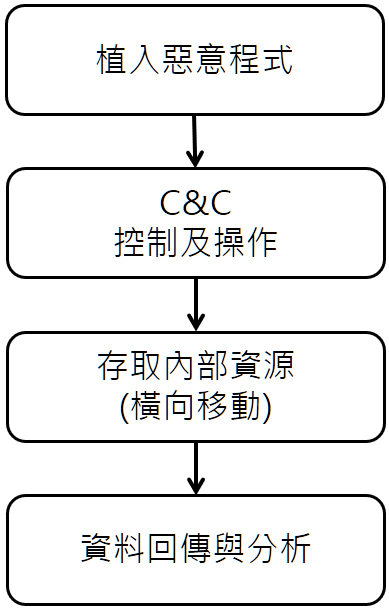
圖15 重設密碼連結設定

第三章 資安新興議題研討

本報告所探討的資安新興議題，包括滲透 Air-Gapped Network 之 Ghost Tunnel 攻擊與 WebDAV 緩衝區溢位漏洞攻擊等議題。

3.1 滲透 Air-Gapped Network 之 Ghost Tunnel 攻擊

Air-Gapped Network[2]是基於網路安全考量，將內部網路與外部網路以物理方式隔離的網路架構。一般而言，駭客是無法由外部網路連線存取已隔離的內部資源，Air-Gapped Network 入侵的來源可能包括供應鏈攻擊、受騙的內部使用者或惡意的內部使用者。攻擊者可在 Air-Gapped Network 內任意一台電腦植入惡意程式，並透過無線電頻率(Radio Frequency)[3]、超聲波[4]、燈光[5]或磁力[6]等傳輸途徑，對受感染之電腦進行控制與資料傳輸，Air-Gapped Network 入侵流程，詳見圖 16。



資料來源：本報告整理

圖16 Air-Gapped Network 入侵流程

Ghost Tunnel[7]是一種可應用於上述隔離網路的後門傳輸方式，並在使用者不知情的情況下，對目標進行控制與訊息回傳。以下將說明 Ghost

Tunnel 如何利用 WiFi 無線連網功能的特性，對 Air-Gapped Network 進行攻擊。

3.1.1 Ghost Tunnel 說明

目前智慧型手機、筆記型電腦、物聯網(Internet of Things，以下簡稱 IoT)裝置及個人電腦幾乎都有 WiFi 無線連網功能。在 802.11 傳輸協定(WiFi)中，Ghost Tunnel 可在使用者自行定義的變數中，塞入惡意程式間用來溝通的 payload，達成資料傳輸目的。

●Ghost Tunnel 特性

– 調用系統提供給 WiFi 廠商的應用程式介面(Application Programming Interface，以下簡稱 API)，可避開防毒及防火牆偵測。

– 不受作業系統限制。

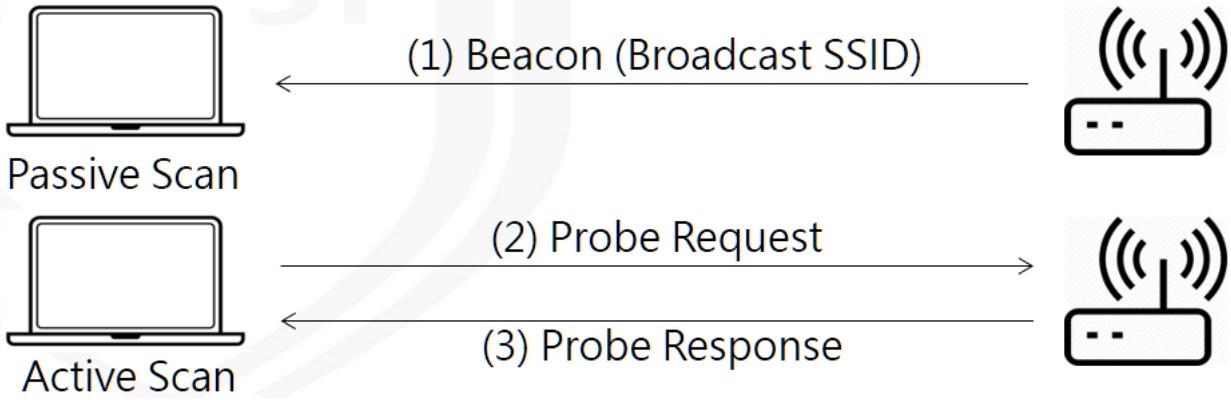
– 同時可控制數量為 256 台。

– 連線有效範圍約 50 公尺。

●設備進行 WiFi 連接時，有以下 2 種方式，其連接方式詳見圖 17。

●設備進行被動式掃描時，會尋找由接取點(Access Point，以下簡稱 AP)或 ad hoc 設備所產生的 Beacon，使用者點選欲連上的 AP，則傳出 Probe request 試著與網路結合。

– 設備進行主動式掃描時，會發出包括服務設定識別碼(SSID)的 Probe request，若找到相同 SSID 的 AP，則 AP 會回應 Probe response 完成確認，並進行連線的下一個步驟。



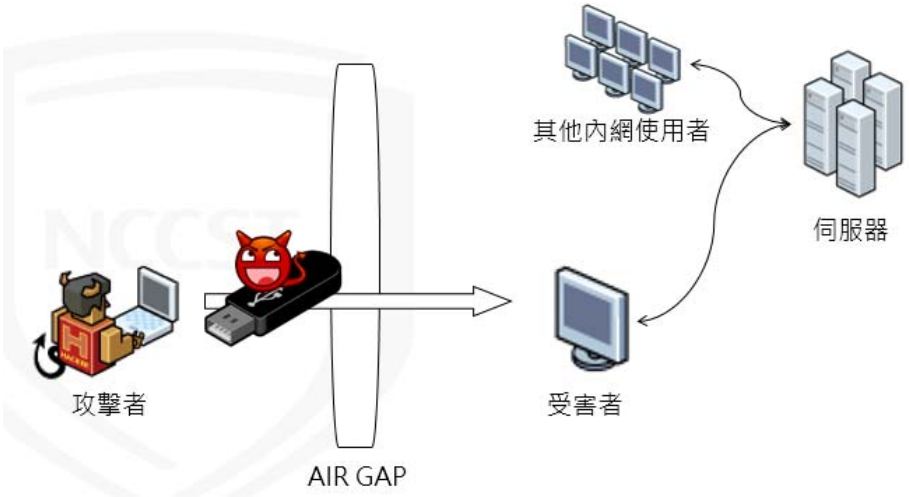
資料來源：本報告整理

圖17 設備與 WiFi 連接示意

3.1.2 Ghost Tunnel 攻擊手法

以下將說明在 Air-Gapped Network 環境，Ghost Tunnel 的攻擊手法。

- 步驟一：攻擊者利用隨身碟或社交工程，在受害者電腦中植入 Ghost Tunnel 的惡意程式，詳見圖 18。



資料來源：本報告整理

圖18 利用隨身碟或社交工程植入惡意程式

- 步驟二：攻擊者造一個隱藏的假 AP，並用特定的 SSID 進行識別，詳見圖 19。

資料來源：本報告整理

圖19 利用偽冒 AP 誘騙受害者連線

●步驟三：攻擊者開啟 Ghost Tunnel Server，與受害者電腦進行連線，詳見圖 20。

資料來源：本報告整理

圖20 開啟 Ghost Tunnel Server 進行連線

透過上述步驟即可在受害者沒有任何的網路連線，但有開啟 WiFi 功能的情況下，利用被植入的 Ghost Tunnel 惡意程式來建立後門溝通管道。

由於 Ghost Tunnel 在建立與攻擊者之溝通管道的時機點為惡意程式植入

後、WiFi 連線建立前，因此具有容易隱藏且難以發現之特性。雖然目前使用之 Air-Gapped Network 架構的資訊環境已可阻絕大部分的攻擊，但不意味著絕對安全，資訊人員仍須提高資安意識。對於運用在機敏環境的 Air-Gapped Network，除要修復系統與軟體的漏洞，還須嚴加控管一切不被信任的外部媒體儲存裝置與硬體設備，以降低風險發生的可能性。

3.2 WebDAV 緩衝區溢位漏洞攻擊

行政院資通安全會報技術服務中心(以下簡稱技服中心)發現駭客利用 WebDAV(Web-Based Distributed Authoring and Versioning，以下簡稱 WebDAV)之 CVE-2017-7269 漏洞攻擊政府機關，並植入駭客工具。為協助政府機關加強防護作為，進一步研析 CVE-2017-7269 漏洞，以掌握漏洞影響範圍，並提供相關防護建議。

3.2.1 WebDAV 簡介

WebDAV 為 HTTP 延伸的協定，提供遠端維護網站資料服務，使用者可透過具 WebDAV 協定之工具，遠端管理網站/系統文件，詳見圖 21。

資料來源：本報告整理

圖21 透過具 WebDAV 協定之工具遠端管理功能

WebDAV 擴充標準 HTTP 的指令與 HTTP 標頭，增加的指令詳見表 5。

表5　WebDAV 增加的指令

項次	Method	說明
1	COPY	將資源從 A 位址複製到 B 位址
2	MOVE	將資源從 A 位址移動到 B 位址
3	LOCK	鎖定資源以防止多個使用者同時修改
4	UNLOCK	解除鎖定的資源
5	MKCOL	創建目錄
6	PROPPATCH	修改資源屬性
7	PROPFIND	擷取資源屬性或目錄結構

資料來源：本報告整理

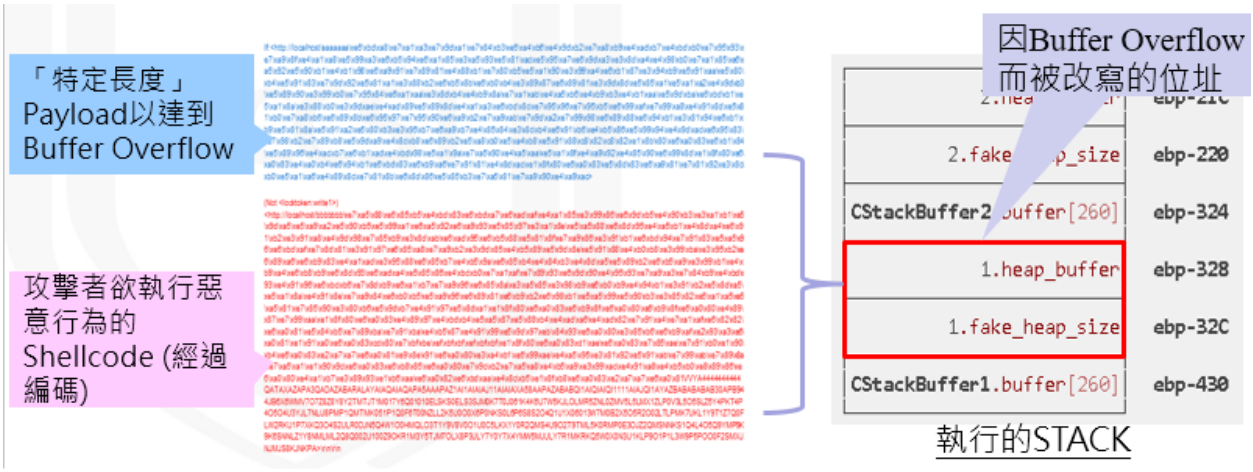
以下將探討 PROPFIND 所呼叫的函式中，存在攻擊者可造成系統緩衝區溢位(Buffer Overflow)，進而遠端執行命令的漏洞。

3.2.2 緩衝區溢位漏洞攻擊說明

CVE-2017-7269 為 WebDAV 服務存在緩衝區溢位弱點，允許攻擊者遠端執行任意程式碼或造成阻斷服務的安全漏洞。作業系統版本為 Microsoft Windows Server 2003 R2、使用 IIS 6.0，又開啟 WebDAV 服務之伺服器，就有可能被利用此漏洞攻擊。攻擊特徵為網站伺服器 Log 中會出現大量的 PROPFIND，觸發函數為 ScStoragePathFromUrl 函數。

首先，WebDAV 的 PROPFIND 功能會呼叫 HrCheckIfHeader 函式，其中呼叫另一個函式 ScStoragePathFromUrl 時未針對字串長度進行檢查，導致駭客可利用 Buffer Overflow 漏洞進行攻擊，之後攻擊者可在 PROPFIND 請求中，植入計算與編碼過後的 Payload 於特定位址(fake_heap_size,

heap_buffer)。在第二次呼叫 ScStoragePathFromUrl 函式時，攻擊者可在 Payload 前段植入欲改寫的部分位址以覆蓋正常位址，在解析後段 Payload 時，資料會寫進被改寫後的位址(惡意 Shellcode)，詳見圖 22。



資料來源：本報告整理

圖22 駭客利用 Buffer Overflow 漏洞進行攻擊手法

全球估計約有 0.6%的網站仍使用 IIS 6.0，WebDAV 為早期駭客常使用入侵網站攻擊手法，政府機關經多次宣導，多數均已關閉此網站服務。雖然透過系統升級方式亦可避免駭客利用該攻擊手法，惟部分機關因資源不足，無法即時升級作業系統。若已啟用 WebDAV，除可透過 IIS 管理員禁止該功能外，亦可修改機碼關閉該功能。執行 Regedit 於「HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters」加入以下 registry value，Value name：DisableWebDAV，Data type：DWORD，Value data：1，之後重新開啟 IIS 服務即可套用新設定。若需再次啟用 WebDAV，則將值設為 0 後，重新開啟 IIS 服務即可。

第四章 結論

本報告透過 6 大面向研析本季之全球資安威脅現況，並針對「關鍵資訊基礎設施資安風險倍增」與「資安(訊)供應商持續遭駭破壞供應鏈安全」等 2 大面向，以本季發生的重大資安事件來探討關鍵資訊基礎設施資安風險與供應鏈或供應商因本身弱點可能造成之風險衝擊。在國內部分，分析政府資安威脅現況，發現事件原因以網站設計不當為主，其次分別為其他、弱密碼及應用程式漏洞等。針對本季全球與政府所面臨的主要資安威脅，本報告就「關鍵資訊基礎設施安全之防護」、「身分認證與存取管控安全」及「網站設計不當與弱密碼」等 3 方面，提出資安防護建議。

資安專題分享說明於 107 年 11 月公告的「資通安全責任等級分級辦法」之資通系統防護基準要求之重要控制措施，協助機關了解技術面實作項目。同時特別針對技術面部分說明驗證方法與實作範例，協助機關了解技術面安全性設定，以強化系統安全性，並符合法規要求。

本季資安新興議題探討，針對「滲透 Air-Gapped Network 之 Ghost Tunnel 攻擊」手法，若使用 Air-Gapped Network 可能遭受駭客入侵的可能性，提醒系統管理者除修復系統與軟體的漏洞外，還須控管一切不被信任的外部媒體儲存裝置與硬體設備。另外，介紹「WebDAV 緩衝區溢位漏洞攻擊」駭客入侵手法，藉由實際資安事件研析入侵手法，並掌握漏洞影響範圍與提供相關防護建議。

下一季「資通安全技術報告」，除持續分析全球與國內政府機關之資安威脅現況，以及從蒐集新興資安議題，從國內外情資與相關研究人員角度提供防護重點。另外，由於員工遠距或在家工作及使用家用裝置連網，已逐漸成為網路應用趨勢，組織在面臨員工自帶資訊設備的資安風險亦逐漸提高，故下期資安專題分享主題規劃為物聯網設備漏洞挖掘與分析。

資安相關活動

本季行政院資通安全處辦理多項資安相關活動，活動細節說明如下：

◆ 資安巡迴宣導

為提升政府機關資安管理與技術之認知與技能，每年定期辦理 2 次資安巡迴宣導，107 年第 2 次研討會共辦理 6 場次說明會，主要在宣導最新資安防護重點與訊息。

首先報告「資安威脅趨勢與案例分享」，介紹近期資安威脅趨勢，包括資安攻擊活動分析、進階持續威脅趨勢分析及網路隔離安全威脅等，同時藉由資安事件案例，例如 SCADA HMI 人機界面漏洞利用及智慧科技漏洞利用案例，說明發生原因與解決方案。

另一類主題為因應資安法施行，分別就「因應資安法施行-通報應變網站調整說明」與「因應資安法施行-資訊系統符合資安法規之安全強化說明」，說明通報應變網站之改版與帳號設置等議題，以及資通系統應如何進行強化，以符合資安法之要求。

最後主題為「107 年網路攻防演練重要發現事項」，說明網路攻防演練執行方式與資訊系統實兵演練綜合發現事項。

◆ 資安服務廠商評鑑

資安服務廠商評鑑主要目的在協助政府機關導入優質民間廠商資安服務，強化資安防護能力，了解資安服務廠商能量及專業技術，做為資安作業委外評選合作對象之參考，進而強化與產業之交流互動。

自 102 年起開辦迄今，針對 SOC 監控服務與一般資安服務廠商進行評鑑。從一開始只有 2 家受評廠商，107 年已增加至 14 家廠商接受評鑑。

資安服務評鑑項目包括 SOC 監控、資安健診、滲透測試、弱點掃描及社

交郵件等項目，評鑑方式包括實地評鑑、展示評鑑及問卷評鑑等方式，分別由評鑑委員與採購資安服務之機關，就資安服務廠商之學習成長能力、服務流程能力、專業技術能力、服務品質能力等 4 個構面進行評鑑，評鑑結果公告於技服中心網站。

參考文獻

[1]行政院國家資通安全會報。資通安全責任等級分級辦法。取自：https://nicst.ey.gov.tw/Page/D94EC6EDE9B10E15/8c1e32e1-f068-4cab-a97d-865d5524d705

[2]Ben-Gurion University of the Negev, The Air-Gap Jumpers。取自：https://i.blackhat.com/us-18/Wed-August-8/us-18-Guri-AirGap.pdf

[3]無線電頻率(Radio Frequency)，取自：https://nsa.gov1.info/dni/nsa-ant-catalog/usb/index.html

[4]超聲波, MOSQUITO: Covert Ultrasonic Transmissions between Two Air-Gapped Computers using Speaker-to-Speaker Communication，取自：https://arxiv.org/pdf/1803.03422.pdf

[5]燈光, Ben-Gurion University of the Negev Cyber Security Research Center, xLED: Covert Data Exfiltration from Air-Gapped Networks via Router LEDs，取自：https://arxiv.org/ftp/arxiv/papers/1706/1706.01140.pdf

[6]磁力, Ben-Gurion University of the Negev Cyber Security Research Center, ODINI : Escaping Sensitive Data from Faraday-Caged, Air-Gapped Computers via Magnetic Fields，取自：https://arxiv.org/pdf/1802.02700.pdf

[7]Ghost Tunnel, Ghost Tunnel: Covert Data Exfiltration Channel to Circumvent Air Gapping，取自：https://conference.hitb.org/hitbsecconf2018ams/sessions/ghost-tunnel-covert-data-exfiltration-channel-to-circumvent-air-gapping/#