麗林國小資安事件通知記錄							
序號	日期	編號	影響等	事故類	內容	影響平	建議措施
01	108/03/29	TACERT-ANA-2019032708032323	高	ANA-漏洞預警	【漏洞預警】Mozilla Firefox瀏覽器存在安全漏洞(CVE-2019-9810與CVE-2019-9813)，允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新	1.Mozilla Firefox 66.0(含)以前版本 2.Mozilla Firefox ESR 60.6.0(含)以前版	[建議措施:] 1.請確認瀏覽器版本，點擊瀏覽器選單按鈕，點選「說明」-->「關於Firefox」，可查看當前使用的Mozilla Firefox瀏覽器是否為受影響之版本 2.更新方式如下： (1)開啟瀏覽器，點擊選單按鈕，點選「說明」-->「關於Firefox」，瀏覽器將執行版本檢查與更新 (2)點擊「重新啟動以更新Firefox」完成更新 3.保持良好使用習慣，請勿點擊來路不明的網址連結
02	108/04/19	TACERT-	低	ANA-漏洞	轉發 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-ANA-201904-0002 華碩電腦於108年3月26日在官方網站表示，其自動更新軟體ASUS Live Update工具程式，遭駭客植入惡意程式碼進行攻擊。 為避免資安疑慮，建議各單位檢視內部使用之華碩裝置是否使用ASUS Live Update工具程式，並將其更新至最新版本(V3.6.8或是更高的版本)。 此訊息僅發送到「區縣市網路中心」，煩請貴單位協助公告或轉發	使用ASUS Live Update工具程式之作業平台	[建議措施:] 1.確認機關使用之華碩電腦是否搭載ASUS Live Update工具，並至華碩官方網站(https://www.asus.com/tw/News/IsyIB2Q5VN9N1Y3w)，使用其提供的檢測程式確認電腦是否受害。 2.將電腦中ASUS Live Update更新至V3.6.8或者更高的版本，更新方式可參考華碩官網(https://www.asus.com/tw/support/FAQ/1018727/)。

03	108/05/13	TACERT-ANA-2019051309052222	低	ANA-資安訊息	轉發 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-ANA-201905-0089。 有鑑於個資外洩威脅日增，請加強向各自所屬單位宣導個資管理，並針對保有個人資料之網站(如活動報名系統、專案型系統等)，強化個資安全防護措施，宣導個資保護意識。 此訊息僅發送到「區縣市網路中心」，煩請貴單位協助公告或轉發	N/A	[建議措施:] 1.規劃與落實個資保護安全控制措施。 參考「105年個人資料保護參考指引(V2.0)」中之安全控制措施規劃(3.1.8)與建立安全控制措施(3.2.3)說明，針對個資保護技術安全控制項目進行妥適規劃、評估與量測，以強化個人資料之安全防護。 2.強化委外管理。 如將個人資料委託第三方廠商處理，可參考「107年政府資訊作業委外服務參考指引(修訂)(V5.1)」之個人資料委外管理風險與注意事項(2.5.3)，落實個資保護要求與管理。 3.加強管控網站安全。 針對保有個資之網站應納入管理範圍，妥善保護網站儲存之個人資料。若為短期活動或專案性質，應於活動或專案終止後立即離線關閉，而所包含之個人資料應限制存取，並於個資期限屆滿後落實刪除。 4.重新檢視依法公開之個人資料。 如有因應法規要求而需公開於網站之個人資料，請重新檢視公開內容之妥適性，並增加其上線公布之審查程序，以避免洩露不適當的個人資料。
04	108/05/24	TACERT-ANA-2019051309052222	低	ANA-資安訊息	轉發 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-ANA-201905-0089。有鑑於個資外洩威脅日增，請加強向各自所屬單位宣導個資管理，並針對保有個人資料之網站 (如活動報名系統、專案型系統等)，強化個資安全防護措施，宣導個資保護意識。	N/A	1.規劃與落實個資保護安全控制措施。 參考「105年個人資料保護參考指引(V2.0)」中之安全控制措施規劃(3.1.8)與建立安全控制措施(3.2.3)說明，針對個資保護技術安全控制項目進行妥適規劃、評估與量測，以強化個人資料之安全防護。 2.強化委外管理。 如將個人資料委託第三方廠商處理，可參考「107年政府資訊作業委外服務參考指引(修訂)(V5.1)」之個人資料委外管理風險與注意事項(2.5.3)，落實個資保護要求與管理。 3.加強管控網站安全。 針對保有個資之網站應納入管理範圍，妥善保護網站儲存之個人資料。若為短期活動或專案性質，應於活動或專案終止後立即離線關閉，而所包含之個人資料應限制存取，並於個資期限屆滿後落實刪除。 4.重新檢視依法公開之個人資料。 如有因應法規要求而需公開於網站之個人資料，請重新檢視公開內容之妥適性，並增加其上線公布之審查程序，以避免洩露不適當的個人資料。

05	108/05/28	TACERT-ANA-20190527 09053737	低	ANA-漏洞預警	轉發 台灣電腦網路危機處理暨協調中心 資安訊息警訊 TWCERTCC-ANA-201905-0006 Synology Virtual Machine Manager是協助使用者集中管理多台 Synology NAS的軟體套件。 研究人員發現Synology-SA-19:25 Virtual Machine Manager存在安全漏洞，遠端攻擊者可利用此漏洞，繞過 Virtual Machine Manager 之安	Virtual Machine Manager 2.4 Virtual Machine Manager 2.3	使用 Virtual Machine Manager 套件的單位盡快更新到最新版本 Virtual Machine Manager 2.4 升級到 2.4.1-9259 或更新版本 Virtual Machine Manager 2.3 升級到 2.3.5-9030 或更新版本
06	108/06/10	TACERT-ANA-20190606 01065858	中	ANA-漏洞預警	轉發國家資安資訊分享與分析中心 資安訊息警訊 NISAC-ANA-201906-0027 NUUO NVR是一個以嵌入式Linux為基礎的網路監控錄影系統，可同時管理多個網路攝影機，並將影像回傳至儲存媒體或設備。本中心研究團隊發現多款NUUO NVR產品系統存在安全漏洞(CVE-2019-9653)，攻擊者可繞過身分驗證於目標系統上執行任意程式碼。由於NVR系統之handle_load_config.php頁面缺少驗證與檢查機制，攻擊者可透過發送客製化惡意請求，利用此漏洞以管理者權限(root)遠端執行系統	NUUO NVR相關產品其韌體版本為1.7.x 至3.3.x版本	[建議措施:] 目前京晨科技官方已有較新版本的韌體釋出，建議將韌體版本升級至最新版本： 1.使用官方提供之新版本韌體進行更新，下載連結： https://www.nuuo.com/DownloadMainpage.php 2.針對無法更新之NVR系統，請透過防護設備或系統內部設定限制存取來源，嚴格限制僅管理人員能夠存取系統之handle_load_config.php頁面，並禁止對該頁面發送任何系統指令與傳入特殊字元。

07	108/06/21	TACERT-ANA-20190515 02053333	高	ANA-漏洞預警	轉發 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-ANA-201905-0199 微軟Windows遠端桌面服務(Remote Desktop Services)，在Windows Server 2008前之作業系統中稱為終端服務(Terminal Services)，該服務允許使用者透過網路連線進行遠端操作電腦。研究人員發現遠端桌面服務存在安全漏洞(CVE-2019-0708)，遠端攻擊者可對目標系統之遠端桌面服務發送特製請求，利用此漏洞進而遠端執行任意程式碼。	Windows XP Windows 7 Windows Server 2003 Windows Server 2008 Windows Server 2008 R2	[建議措施:] 目前微軟官方已針對此弱點釋出更新程式，請儘速進行更新： 1.Windows XP與Windows Server 2003作業系統雖已停止支援安全性更新，但微軟仍針對此漏洞釋出更新程式，請至下列連結進行更新：https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708 2.作業系統如為Windows 7、Windows Server 2008及Windows Server 2008 R2，請至下列連結進行更新：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
08	108/06/21	TACERT-ANA-20190515 02053838	低	ANA-漏洞預警	轉發 台灣電腦網路危機處理暨協調中心 資安訊息警訊 TWCERTCC-ANA-201905-0001 TWCERT/CC接獲國外通報，Toshiba 和 Brother 印表機Web Services列印存在安全漏洞，攻擊者可利用進行反射放大DDos攻擊。	Toshiba 和 Brother 印表機	建議停用Web Services列印功能，步驟如下： Toshiba (TopAccess example): 1) Log into Web Interface 2) Go to Administration > Setup > Network 3) Disable Web Services Print 4) Click Save and allow the copiers web server to restart Brother (HL-5470DW model example): 1) Log into Web interface 2) Go to Network > Protocol 3) Uncheck Web Services 4) Click Submit and allow the copiers web server to restart