延宇資訊股份有限公司

機密等級：■一般 □限閱 □密 □機密	文件編號：YAN-ISMS-04-53	保存年限：2年
日期： 115 年 06 月 16 日	紀錄編號：YAN-ISMS-G-53-11506-01	版本：1.0

威脅情資收集與處理記記錄單

登錄人員： 黃韋霖

項次	威脅情資收集日期	威脅情資來源/威脅情資內容	受影響之資通系統	採取相關控制措施								備註
1	115/04/22	TWCERT/CC /研究人員發現Adobe Acrobat Reader存在原型鏈汙染(Prototype Pollution)漏洞(CVE-2026-34621，CVSS：8.6)，未經身分鑑別之攻擊者可誘使使用者開啟特製惡意檔案，污染程式執行時之物件原型，進而於目前使用者權限執行任意程式碼。此漏洞已遭駭客利用，請儘速確認並進行修補。	公司筆電	立即更新程式						蒐集人員	黃韋霖	
										處理人員	黃韋霖	
	向相關關注方通報：■否 □是，關注方通報窗口：_____		通報時間：2026/04/22 通報人員：黃韋霖	預計完成日期	2026/04/22	實際完成日期	2026/04/22	是否列入風險管理	否	主管確認	延宇資訊股份有限公司 梁維志	
2	115/05/22	Palo Alto Networks 的防火牆作業系統 PAN-OS的User-ID驗證入口網站服務存在緩衝區溢位漏洞(CVE-2026-0300，CVSS ：9.3)，此漏洞允許未經身分驗證的攻擊者透過發送特製的資料，在PA系列和VM系統防火牆上，以root權限執行任意程式碼。	公司暫時下架之防火牆PA-440	安排更新防火牆韌體							蒐集人員	黃韋霖	
										處理人員	黃韋霖	
	向相關關注方通報：■否 □是，關注方通報窗口：_____		通報時間：2026/05/22 通報人員：黃韋霖	預計完成日期	115/07/31	實際完成日期		是否列入風險管理	否	主管確認	延宇資訊股份有限公司 梁維志	
3	115/06/02	Palo Alto Networks 防火牆作業系統 PAN-OS的GlobalProtect入口網站和通道設備存在身分驗證繞過漏洞，攻擊者可利用該漏洞繞過安全限制並建立未經授權的VPN連線。	公司暫時下架之防火牆PA-440	安排更新防火牆韌體，已於 7/1 更新完畢						蒐集人員	黃韋霖	
										處理人員	黃韋霖	
	向相關關注方通報：■否 □是，關注方通報窗口：_____		通報時間：2026/06/02 通報人員：黃韋霖	預計完成日期	115/07/31	實際完成日期	115/7/1	是否列入風險管理	否	主管確認	延宇資訊股份有限公司 梁維志	
										蒐集人員		
										處理人員		
	向相關關注方通報：□否 □是，關注方通報窗口：_____		通報時間：_____ 通報人員：_____	預計完成日期		實際完成日期		是否列入風險管理		主管確認		
										蒐集人員		
										處理人員		
	向相關關注方通報：□否 □是，關注方通報窗口：_____		通報時間：_____ 通報人員：_____	預計完成日期		實際完成日期		是否列入風險管理		主管確認		