行政院國家資通安全會報技術服務中心

漏洞/資安訊息警訊

發布編號	NCCST-ANA-2018-0049	發布時間	Wed May 16 15:52:04 CST 2018
事件類型	漏洞預警	發現時間	Tue May 15 00:00:00 CST 2018
警訊名稱	電子郵件 OpenPGP 及 S/MIME 加密規範存在安全漏洞(CVE-2017-17688 與 CVE-2017-17689)，允許攻擊者竊取機敏郵件資訊		
內容說明	OpenPGP 與 S/MIME 是電子郵件端點對端點的加密規範。 研究人員發現 OpenPGP(CVE-2017-17688)及 S/MIME(CVE-2017-17689)存在安全漏洞，攻擊者透過中間人攻擊進行郵件攔截，再以特殊的格式將已加密的段落加上 HTML 的標籤(Tag)，當受害者收到修改的電子郵件並進行解密後會載入外部 HTML 內容，使加密訊息以明文回傳至攻擊者，進而造成機敏郵件資訊外洩等。		
影響平台	所有使用 OpenPGP 及 S/MIME 規範的郵件軟體		
影響等級	高		
建議措施	1.目前 OpenPGP 與 S/MIME 為協定上的邏輯漏洞，目前尚無修補方式，請持續留意相關訊息的發布。 2.此漏洞緩解的方法如下： ・以純文字方式開啟信件，避免以 HTML 讀取信件 ・刪除電子郵件中保存的私鑰，並將密文複製至其他單獨的應用程式進行解密，解密方式可參考以下網址(https://www.eff.org/deeplinks/2018/05/pretty-good-procedures-protecting-your-email) 3.請定期檢視系統/應用程式更新紀錄，避免駭客利用系統/應用程式安全性漏洞進行入侵行為，並更新防毒軟體病毒碼以加強防護。		
參考資料	1. https://efl.de 2. https://securitytracker.com/id/1040904 3. https://securitytracker.com/id/1040906		

	4. https://securitytracker.com/id/1040907

此類通告發送對象為通報應變網站登記之資安人員。若貴 單位之資安人員有變更，可逕自登入通報應變網站（https://www.ncert.nat.gov.tw）進行修改。若您仍為貴單位之資安人員但非本事件之處理人員，請協助將此通告告知相關處理人員。

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。

地 址： 台北市富陽街 116 號
聯絡電話： 02-27339922
傳真電話： 02-27331655
電子郵件信箱： service@nccst.nat.gov.tw