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	ICST-ANA-2009-0004	發布時間	2009/07/29 12:22:40
事件類型	攻擊活動預警	發現時間	2009/07/28
警訊名稱	惡意電子郵件特徵通知		
內容說明	經由遭受惡意電子郵件攻擊之政府機關提供資訊，並由本中心比對已掌握之惡意郵件後確認，有不少比例之惡意郵件會使用 DreamMail 發送，因此在郵件標頭中含有 X-Mailer: DreamMail 特徵。		
影響平台	無特定平台，一般會接收電子郵件之使用者均可能受影響		
影響等級	中		
建議措施	可使用防垃圾郵件軟體或入侵偵測系統，比對郵件標頭是否含有 X-Mailer: DreamMail 特徵，找出潛在之惡意郵件，詳細設定方法依產品而異，請尋求廠商支援。 附註： 1. 攻擊者可任意變換使用之郵件軟體，且並非所有攻擊者均使用這套郵件軟體，因此這個措施並無法偵測所有惡意郵件。 2. DreamMail 爲免費郵件軟體，一般公務上需使用之可能性極低，但仍有可能有使用者習慣使用這套軟體發送正常信件。 3. 建議可先使用偵測模式評估這個措施是否有效，必要時再使用阻擋模式。		
參考資料	無		

此類通告發送對象爲通報應變網站登記之資安聯絡人。若貴 單位之資安聯絡人有變更，可逕自登入通報應變網站（https://www.ncert.nat.gov.tw/）進行修改。若您仍爲貴 單位之資安聯絡人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。

國家資通安全會報 技術服務中心 (http://www.icst.org.tw/)
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@icst.org.tw