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-2021-0000143	發布時間	Tue Apr 27 16:32:07 CST 2021
事件類型	攻擊活動預警	發現時間	Mon Apr 26 00:00:00 CST 2021
警訊名稱	[更新附件]駭客針對 ArmorX LisoMail 郵件系統進行 XSS 跨網站指令碼攻擊行動預警		
內容說明	本中心接獲外部情資發現近期駭客組織攻擊活動頻繁，駭客針對 ArmorX LisoMail 郵件系統之登入網頁(webmail2)進行跨網站指令碼(Cross-Site Scripting, XSS)攻擊後植入網頁後門程式，並竊取系統之使用者帳號與密碼，後門程式路徑如下： /dev/shm/usr/isb/html/webmail2/program/lib/xml.php /dev/shm/usr/isb/html/webmail2/program/lib/tunnel.php 各機關應提高警覺，若有採購/使用該系統應儘速完成原廠作業系統版本更新，並落實監控防護與異常連線阻擋，如於相關日誌發現異常連線或警示，應深入釐清事件原因與影響範圍，避免錯失調查時機。		
影響平台	ArmorX LisoMail 郵件系統 2020/12/31 之前的所有版本 (版本識別碼 8.15.2-2.712.063-1.90.013)		
影響等級	中		
建議措施	1. 檢視是否使用上述設備或產品並確認其修補或更新狀態，若未進行修補或更新應儘速完成，避免未來可能被作為攻擊之對象。 2. 清查監控紀錄以釐清是否曾經發生異常事件。 3. 依據附件所列之 IP 與 DN 等 IoC 資訊，加強監控防護與異常連線阻擋。		
參考資料	1. http://www.armorx.com.tw/update.html#2020-12-31 2. 請參考附件。		

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