

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-2017-0025	發布時間	Tue Mar 07 22:46:23 CST 2017
事件類型	公告資訊	發現時間	Tue Mar 07 00:00:00 CST 2017
警訊名稱	特定版本 Apache Struts 2 存在允許攻擊者遠端執行任意程式碼之漏洞(CVE-2017-5638)，請儘速確認並進行修正。		
內容說明	Apache Struts 2 是一個開放原始碼的 Java EE 網站應用程式的 Web 應用框架。 該漏洞主要是 Apache Struts 2 負責處理檔案上傳封包的 Jakarta 解析程式(parser)存在安全性漏洞，遠端攻擊者可利用漏洞寄送含有惡意 Content-Type 值的封包，造成攻擊者可遠端執行任意程式碼，進而可能導致機敏資訊外洩等風險。		
影響平台	Apache Struts 2.3.5 至 2.3.31 的版本 Apache Struts 2.5 至 2.5.10 的版本		
影響等級	高		
建議措施	1.請各機關應確認網站主機是否使用 Apache Struts 2 的網頁應用框架，可透過檢查網站主機目錄中「WEB-INF\lib\」資料夾內的 Struts2.jar 檔，確認當前使用的版本。 2.如所使用的 Apache Struts 2 為上述(2.3.5 至 2.3.31 或 2.5 至 2.5.10)受影響之版本，則請更新官方 Github 所釋出最新之 Apache Struts 2.3.32 或 Struts 2.5.10.1 的版本。		
參考資料	1. https://cwiki.apache.org/confluence/display/WW/S2-045 2. https://github.com/apache/struts/releases		

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