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-2017-0089	發布時間	Wed Sep 06 17:13:18 CST 2017
事件類型	漏洞預警	發現時間	Wed Sep 06 00:00:00 CST 2017
警訊名稱	[更新-建議措施第 2、3]Apache Struts 2.5 至 2.5.12 版本中的 REST 套件存在允許攻擊者遠端執行任意程式碼之漏洞(CVE-2017-9805)，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 網路應用程式的 Web 應用框架，REST(Representational State Transfer)則是一種全球資訊網軟體架構風格，可便於不同軟體或程式在網路中互相傳遞資訊。 Apache Struts 2 中的 REST 套件提供開發者可遵循 REST 的理念與原則進行程式開發，該漏洞主要是在 Apache Struts 2.5 至 2.5.12 版本中，當使用 REST 套件之 XStream 處理程序針對 XML 請求進行反序列化時，因未進行類型過濾，可能導致攻擊者可傳送惡意的 XML 封包，進而造成遠端執行任意程式碼與控制系統。		
影響平台	Apache Struts 2.5 至 2.5.12 版本		
影響等級	高		
建議措施	1.目前 Apache 官方已針對此弱點釋出修復版本，請儘速至官方網頁 (https://struts.apache.org/download.cgi#struts2513)進行更新。 [更新]2.如無使用 REST 套件需求，請刪除 REST 套件。確認方式於 WEB-INF\lib 目錄下是否有 struts2-rest-plugin-2.x.jar 檔案。 [更新]3.如需在受影響平台中持續使用 REST 套件，可於 REST 套件內的 struts-plugin.xml 設定檔中，依官方網頁(https://struts.apache.org/docs/s2-052.html)所提供之解決方案進行內容新增，可降低此漏洞影響程度。		
參考資料	1.https://struts.apache.org/docs/s2-052.html 2.https://github.com/apache/struts/blob/bbd4a9e8c567265c0eb376c0f8a3445f4d9a5fdf/plugins/rest/src/main/resources/struts-plugin.xml 3.http://thehackernews.com/2017/09/apache-struts-vulnerability.html		

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