張貼日期：2017/09/08

[資安漏洞預警通知] 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

主旨□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

說明：

1. 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。
2. 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。
3. 影響平臺□ Apache Struts 2.5至2.5.12版本
4. 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。
    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。
    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。
5. 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

---

計算機與通訊中心
網路系統組 敬啟