**From:** 國家資通安全科技中心
**Sent:** Friday, April 29, 2016 11:13 AM
**To:** ncert@nccst.nat.gov.tw
**Subject:** [資安訊息警訊] 國家資通安全科技中心（事件編號：NCCST-ANA-2016-0041)

# 國家資通安全會報 國家資通安全科技中心

# 漏洞/資安訊息警訊

| | | | |
|---|---|---|---|
| 發布編號 | NCCST-ANA-2016-0041 | 發布時間 | Fri Apr 29 10:34:07 CST 2016 |
| 事件類型 | 漏洞預警 | 發現時間 | Tue Apr 26 00:00:00 CST 2016 |
| 警訊名稱 | [更新]特定版本 Apache Struts 2 允許攻擊者遠端執行任意程式碼 | | |
| 內容說明 | 根據美國國家標準技術研究所（NIST）的國家弱點資料庫（NVD）發布弱點編號 CVE-2016-3081。[1][2]<br><br>針對 Apache 的 Struts 2.3.20 至 Struts 2.3.28(2.3.20.2、2.3.24.2 除外)版本，攻擊者可透過 DefaultAction.java 的 invokeAction 弱點，將惡意攻擊程式碼夾帶於 Request 中，允許攻擊者遠端執行任意程式碼。[3]<br><br>請各機關檢視所支援的 Apache Struts 2 版本，儘速更新至最新版本。 | | |
| 影響平台 | Apache Struts 2.3.20 至 Apache Struts 2.3.28(2.3.20.2、2.3.24.2 除外) [4] | | |
| 影響等級 | 高 | | |
| 建議措施 | Apache Struts 2.3.20 至 Apache Struts 2.3.28(2.3.20.2、2.3.24.2 除外)版本已發現存在安全漏洞，請各機關確認網站主機是否使用 Apache Struts 2 Web 應用框架。若有使用受影響之版本，請將 Apache Struts 2 更新至 2.3.20.2、2.3.24.2 或 2.3.28.1 以上之版本。[5]<br><br>(1) 檢查是否使用 Apache Struts 2 Web 應用框架，可透過檢查網站主機目錄中的「WEB-INF\lib\」資料夾是否存有 struts 相關 jar 檔，若存有相關 jar 檔再進行版本確認。<br><br>(2) 若選擇不將 Apache Struts 2 更新至 2.3.20.2、2.3.24.2 或 2.3.28.1 以上之版本，應於 struts.xml 設定檔中將「struts.enable.DynamicMethodInvocation」的值設定為「false」，以停用 Dynamic Method Invocation。[6] | | |

| | |
|---|---|
| | (3) 停用 Dynamic Method Invocation 參考設定如下：<br><br><constant name="struts.enable.DynamicMethodInvocation" value="false"/> |
| 參考資料 | 1. https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3081<br><br>2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3081<br><br>3. http://www.securitytracker.com/id/1035665<br><br>4. https://vuldb.com/?id.82790<br><br>5. http://struts.apache.org/download.cgi#struts-ga<br><br>6. https://struts.apache.org/docs/s2-032.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。國家資通安全科技中心 (https://www.ncert.nat.gov.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@nccst.nat.gov.tw