

張貼日期：2016/04/29

轉發漏洞/資安訊息警訊

主旨：【漏洞預警】特定版本Apache Struts 2允許攻擊者遠端執行任意程式碼

說明：

- 轉發行政法人國家資通安全科技中心 資安訊息警訊 NCCST-ANA-201604-0047
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]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]
請各單位檢視所支援的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]
- 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]
(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。
(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：
- 參考資料:
 - <https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3081>
 - <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3081>
 - <http://www.securitytracker.com/id/1035665>
 - <https://vuldb.com/?id.82790>
 - <http://struts.apache.org/download.cgi#struts-ga>
 - <https://struts.apache.org/docs/s2-032.html>

計算機與通訊中心
網路系統組 敬啟

From:
<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:
https://net.nthu.edu.tw/netsys/mailling:announcement:20160429_01

Last update: **2016/04/29 11:46**

