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-2019-0027	發布時間	Wed Mar 13 16:41:05 CST 2019
事件類型	漏洞預警	發現時間	Mon Mar 11 00:00:00 CST 2019
警訊名稱	Apache Solr 存在安全漏洞(CVE-2019-0192)，允許攻擊者遠端執行任意程式碼，請儘速確認並進行更新		
內容說明	Apache Solr 是開放原始碼的全文檢索伺服器，以 Lucene 程式庫為核心，進行全文資料的解析、索引及搜尋。 研究人員發現，Solr 的 ConfigAPI 允許攻擊者透過 HTTP POST 請求修改 jmx.serviceUrl 內容，將 JMX 伺服器指向惡意 RMI/LDAP 伺服器，再運用 Solr 不安全的反序列化功能(ObjectInputStream)，進而導致遠端執行任意程式碼。		
影響平台	?Apache Solr 5.0.0 至 5.5.5 版本 ?Apache Solr 6.0.0 至 6.6.5 版本		
影響等級	高		
建議措施	目前 Apache 官方已針對此弱點釋出修復版本，請各機關可聯絡系統維護廠商或參考以下建議進行： 1.更新時，建議進行測試後再安裝更新 2.可於系統輸入指令「solr version」確認目前使用的版本。若為上述受影響版本，可採取下列措施： (1).更新 Apache Solr 至 7.0 以後版本 (2).若無法立即更新 Solr 版本，可進行下列替代措施： a.停用 ConfigAPI：請執行 Solr 並開啟系統屬性，將 disable.configEdit 設置為 true		

	b.下載 SOLR-13301.patch 並且重新編譯 Solr，下載連結網址如下：https://issues.apache.org/jira/secure/attachment/12961503/12961503_SOLR-13301.patch c.只允許受信任的來源電腦存取 Solr 伺服器
參考資料	1. https://issues.apache.org/jira/browse/SOLR-13301 2. https://vulmon.com/vulnerabilitydetails?qid=CVE-2019-0192 3. http://mail-archives.us.apache.org/mod_mbox/www-announce/201903.mbox/%3CCAECwjAV1buZwg%2BMcV9EAQ19MeAWztPVJYD4zGK8kQdADFYij1w%40mail.gmail.com%3E

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