張貼日期：2019/03/07

[資安漏洞預警通知] 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

主旨：[資安漏洞預警通知] 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:
  - ApacheSolr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
- 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：
          1. 停用ConfigAPI□請執行Solr並開啟系統屬性，將disable.configEdit設置為true
          2. 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
          3. 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

計算機與通訊中心
網路系統組 敬啟