張貼日期：2018/05/18

［資安漏洞預警通知] Spring Framework存在安全漏洞(CVE-2018-1258與CVE-2018-1260)允許攻擊者繞過認證與存取系統上所限制的方法、或是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] Spring Framework存在安全漏洞(CVE-2018-1258與CVE-2018-1260)允許攻擊者繞過認證與存取系統上所限制的方法、或是遠端執行任意程式碼，請儘速確認並進行更新

說明：

- Spring Framework是一個開源的Java/Java EE的Full-Stack應用程式框架Spring Security以及Spring Security OAuth2是一個認證與存取控制的應用程式框架。
- 研究人員發現Spring Framework存在多個安全漏洞，其中又以(CVE-2018-1258與CVE-2018-1260)兩個安全漏洞最為嚴重，允許未經授權的遠端攻擊者繞過認證與存取系統上所限制的方法，或是遠端執行任意程式碼。
- 影響平臺：
  1. CVE-2018-1258
     - Spring Framework 5.0.5
     - Spring Security 5.0.4(含)之前的所有版本
  2. CVE-2018-1260
     - Spring Security OAuth 2.3至2.3.2
     - Spring Security OAuth 2.2至2.2.1
     - Spring Security OAuth 2.1至2.1.1
     - Spring Security OAuth 2.0至2.0.14
     - Spring Security OAuth 1的所有版本
- 建議措施：
  1. Spring Security OAuth 1的所有版本
     - Spring Framework請至以下連結更新至5.0.6版以上：
       1. https://projects.spring.io/spring-framework/
       2. https://github.com/spring-projects/spring-framework/releases/tag/v5.0.6RELEASE
     - Spring Security請至以下連結更新至5.0.5版以上：
       1. https://projects.spring.io/spring-security/
       2. https://github.com/spring-projects/spring-security/releases/tag/5.0.5.RELEASE
     - Spring Security OAuth請至以下連結進行更新：
       1. 2.3.x請至以下連結更新
          至2.3.3：https://github.com/spring-projects/spring-security-oauth/releases/tag/2.3.3RELEASE
       2. 2.2.x請至以下連結更新
          至2.2.2：https://github.com/spring-projects/spring-security-oauth/releases/tag/2.2.2RELEASE
       3. 2.1.x請至以下連結更新
          至2.1.2：https://github.com/spring-projects/spring-security-oauth/releases/tag/2.1.2RELEASE
       4. 2.0.x請至以下連結更新
          至2.0.15：https://github.com/spring-projects/spring-security-oauth/releases/tag/2.0.15.RELEASE
  2. 請定期檢視系統/應用程式更新紀錄，避免駭客利用系統/應用程式安全性漏洞進行入侵行為，亦須更新防毒軟體病毒碼以加強防護。

- 參考資料:
  1. https://pivotal.io/security/cve-2018-1258
  2. https://tools.cisco.com/security/center/viewAlert.x?alertId=57883
  3. https://pivotal.io/security/cve-2018-1260

計算機與通訊中心
網路系統組 敬啟