**何謂OpenSSL，其弱點、影響範圍及防護建議?**

 資料來源：資通安全處

OpenSSL是以Eric Young與Tim Hudson所寫的SSLeay為基礎之開放原始碼SSL套件，主要功能為基本的傳輸層資料加密。在2012/3/14推出的1.0.1版本存在高風險漏洞(漏洞編號：CVE-2014-0160)，漏洞與OpenSSL TLS/DTLS傳輸層安全協議heartbeat擴充元件相關，因此又被稱為Heartbleed漏洞，該漏洞允許攻擊者從伺服器記憶體中讀取最多64KB的資料，將造成記憶體內容外洩風險。  
漏洞資訊  
漏洞編號：CVE-2014-0160  
影響OpenSSL版本：  
OpenSSL 1.0.1~1.0.1f版本  
OpenSSL 1.0.2-beta~1.0.2-beta1版本  
影響系統版本：安裝有漏洞版本OpenSSL的任意作業系統與套件  
可能風險：  
攻擊者利用該漏洞無需通過權限或身份驗證，即可讀取伺服器記憶體，竊取SSL私密金鑰、Session cookie或使用者帳號密碼等機敏資訊。  
攻擊者可針對由OpenSSL保護的網路通信進行解密、偽冒或進行中間人攻擊，以竊取E-mail、文件及通訊內容等，進而入侵伺服器取得機敏資訊。  
詳細內容請連結技術服務中心網站參考http://www.icst.org.tw/Heartbleed.aspx?lang=zh