(一) OpenSSL Heartbleed 漏洞說明:

全球大多數網站使用的伺服器加密程式出現安全漏洞，臉書（Facebook）與雅虎（Yahoo）旗下的部落格網站 Tumblr 建議使用者更改密碼，因為 OpenSSL Heartbleed 的程式安全漏洞漏洞讓攻擊者從伺服器記憶體中擷取記憶體中存在的機敏資料，可能導致伺服器遭到入侵或取得使用者帳密，導致個資外洩。

參考資訊

http://devco.re/blog/2014/04/09/openssl-heartbleed-CVE-2014-0160/

(二) 因應 OpenSSL Heartbleed 漏洞，TANet 區網中心已採取因應措施：

TANet 台大區網中心在第一時間啟動 IPS(Intrusion Prevention System)防護防線，偵測與阻擋 OpenSSL 的漏洞攻擊。

(三) 使用者與管理者的建議措施:

1. 使用者應對措施:

(1). 若常用的網站服務有此漏洞的風險，注意網站是否有更新措施，並請更換密碼。

(2). 若近期有網站通知更換密碼，也請注意是否為釣魚信件。

(3). 注意自己的帳號是否有異常活動。

2. 系統管理者應對措施:

(1). 更新 OpenSSL 至 1.0.1g 或 1.0.2-beta2，並密切注意有無後續更新。

(2). 重新產生金鑰(Private Key 可能外洩)、Session(Session ID 可能外洩) 、密碼 (密碼也可能外洩) ，並且撤銷原本的金鑰。

(3). 若無法更新，重新編譯 OpenSSL 以關閉 heartbeat 功能。

(4). 使用 Perfect Forward Secrecy (PFS)，在未來類似風險發生時減低傷害。