資安訊息：四月份網路安全威脅報告

2014/05/15

風險： 資安訊息

摘　　要：資安事件：綜觀本月份資安新聞，佔據最多版面的不外乎為 OpenSSL Heartbleed 弱點，可參考 iThome 發佈「OpenSSL 重大漏洞 Heartbleed　全球網路加密傳輸安全拉警報」、「資安專家：Heartbleed 是網路有史以來最嚴重的臭蟲」、「SANS 資安專家：小心 HeartBleed 威脅無所不在！」、「使用網路銀行安全嗎？臺灣網路銀行 Heartbleed 災情大清查」及資安人發佈「OpenSSL 傳重大漏洞 台灣知名網站修復龜速」。中華電信 SOC 已有發佈 HiNet 全球預警情報網 OpenSSL 事件通告，建議管理者應儘速確認主機是否使用影響範圍內的 OpenSSL 版本，並請盡速評估是否更新至 OpenSSL 1.0.1g 或 1.0.2beta2 版本，或先關閉 HeartBeat 查詢，以避免遭受此攻擊。安全專家另外建議使用者變更在 2011 年 3 月以後在各種網路服務上所使用的任何密碼，降低帳密外洩後使惡意人士仍可繼續使用的機率。

重大弱點：微軟公佈了 4 項重大更新，Adobe 發布旗下產品(Flash Player /Air /Reader) 共 4 個弱點通告，Apple 發佈旗下產品(Safari /iOS /TV /AirPort /OS X) 共 5 個弱點通告，Google 發佈 Chrome 瀏覽器共 3 個弱點通告，McAfee 發布 5 個弱點通告，Mozilla 發布旗下產品(Firefox /SeaMonkey /Thunderbird) 共 3 個弱點通告，WordPress 發布 12 個弱點通告，Apache 發布 2 個弱點通告，Oracle 發布 24 個弱點通告，Cisco 發佈旗下產品 23 個弱點通告，SUSE 發佈 15 項更新，Red Hat 發布 27 項更新，建議受影響的用戶盡速上網修補。

病毒狀況：防毒軟體廠商近期發現 RTKT_NECURS.BGSG 木馬程式(Microsoft 命名為 Trojan:WinNT/Necurs.A)，是一個透過惡意軟體或檔案下載方式感染的間諜木馬。該木馬會透過 TSPY_ZBOT.YYJR 進行傳播，它會執行所下載的惡意程式，以及在特定登錄機碼下建立登錄項目，並將重要驅動程式設定不可使用。建議您勿瀏覽可疑或惡意網站

以及開啟任何可疑的檔案或郵件，並更新防毒軟體病毒碼至最新版本。

本資訊轉自教育部資安服務網