國家資通安全會報 技術服務中心

漏洞/資安訊息警訊

發布編號	ICST-ANA-2014-0006	發布時間	Fri Apr 11 19:15:02 CST 2014
事件類型	漏洞預警	發現時間	Wed Apr 09 00:00:00 CST 2014
警訊名稱	OpenSSL 存在高風險 CVE-2014-0160 漏洞		
內容說明	OpenSSL 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，因此漏洞又被稱為 heartbleed 漏洞，將造成記憶體內容外洩風險。 攻擊者利用該漏洞無需通過權限或身分驗證，即可讀取伺服器記憶體，竊取 x.509 加密金鑰、使用者帳號密碼、cookies 等，將可對 OpenSSL 保護的網路通信進行解密、偽冒或進行中間人攻擊，竊取 e-mail、文件及通訊內容等機敏資訊。		
影響平台	影響平台： 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：安裝有弱點版本 OpenSSL 的任意作業系統		
影響等級	高		
建議措施	1.安裝有 OpenSSL 的主機可於登入後執行 openssl version 指令確認使用 OpenSSL 版本是否為受影響版本。 2.OpenSSL 已釋出相關修補程式： OpenSSL 版本 1.0.1 系列 - 更新至版本 1.0.1g。 OpenSSL 版本 1.0.2-beta1 - 更新至版本 1.0.2-beta2。(截至 4/11 官網尚未釋出，請再注意官網更新) 修補程式詳見：https://www.openssl.org/source/		
參考資料	參考資料： http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160 https://www.openssl.org/news/secadv_20140407.txt		

	http://heartbleed.com/ http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160 http://www.securityfocus.com/bid/66690/info

此類通告發送對象為通報應變網站登記之資安人員。若貴 單位之資安人員有變更，可逕自登入通報應變網站（https://www.ncert.nat.gov.tw）進行修改。若您仍為貴單位之資安人員但非本事件之處理人員，請協助將此通告告知相關處理人員。

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。國家資通安全會報 技術服務中心 (http://www.icst.org.tw/)

地 址： 台北市富陽街 116 號
聯絡電話： 02-27339922
傳真電話： 02-27331655
電子郵件信箱： service@icst.org.tw