From: 國家資通安全會報技術服務中心
Sent: Tuesday, March 08, 2016 11:58 AM
To: ncert@icst.org.tw
Subject: [資安訊息警訊] 國家資通安全會報技術服務中心 (事件編號 : ICST-ANA-2016-0022)

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-2016-0022	發布時間	Tue Mar 08 11:22:25 CST 2016
事件類型	漏洞預警	發現時間	Tue Mar 08 00:00:00 CST 2016
警訊名稱	關閉不安全的通訊協定 SSLv2，避免遭受中間人攻擊		
內容說明	近期國際資安專家研究發現 SSLv2 具 DROWN(Decrypting RSA with Obsolete and Weakened eNcryption，CVE-2016-0800)[1]安全性漏洞，其主要原因為 SSLv2 設計不當，導致存在安全威脅，包含： 1.同一密鑰(Secret Key)用於訊息身分驗證與加密。 2.認證密文(Cipher)只支援不安全的 MD5 雜湊值。		

	3.利用修改 ClientHello 與 ServerHello 封包，造成中間人(Man In the Middle, MItM)攻擊。 目前大多數瀏覽器、網頁伺服器(HTTPS)及郵件伺服器(SMTPS)均建議不採用 SSLv2 協定[2][3]，避免遭受可能風險如： 攻擊者可利用 SSLv2 協定的安全性漏洞，破解金鑰交換加密演算法，以取得加密金鑰，進而還原加密封包，解析通訊內容。
影響平台	支援 SSLv2 加密通訊協定之伺服器
影響等級	高
建議措施	請各機關檢查 SSLv2 協定使用狀態，並依照修補方式關閉 SSLv2 協定(建議一併關閉 SSLv3)： 使用者端瀏覽器確認與關閉流程(以 IE 為例) 1.點選右上角齒輪，再選擇『網際網路選項』。 2.切換到『進階』頁籤，將畫面往下拉，取消『使用 SSL 2.0』選項(建議亦將『使用 SSL 3.0』取消)，並勾選『使用 TLS 1.0』、『使用 TLS 1.1』、『使用 TLS 1.2』。 伺服器端

	1.伺服器端檢測方式 以下檢測方法採用 Nmap 工具，各機關可透過該工具自行檢測。 指令如下： nmap --script sslv2 -p 443 (若有使用 SSLv2 將會出現以下字串) sslv2: server still supports SSLv2 2.伺服器端修補方式(Tomcat、Apache 以及 IIS 為例) 【Tomcat 修補方式】可透過設定「sslProtocols」或「sslEnabledProtocols」參數，利用白名單方式，關閉 SSL[4]。 Tomcat 5 and 6 (6.0.38 以前版本號)： maxThreads="150" SSLEnabled="true" scheme="https" secure="true" clientAuth="false" sslProtocols = "TLSv1,TLSv1.1,TLSv1.2" /> Tomcat 6 (6.0.38 之後的版本號) 與 7：

	maxThreads="150" SSLEnabled="true" scheme="https" secure="tr ue" clientAuth="false" sslEnabledProtocols = "TLSv1,TLSv1.1,TLSv1.2" /> Tomcat APR： maxThreads="150" enableLookups="false" disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true" SSLEnabled="true" SSLCertificateFile="${catalina.base}/conf/localhost.crt" SSLCertificateKeyFile="${catalina.base}/conf/localhost.key" SSLProtocol="TLSv1"/> 【Apache 修補方式】於 httpd.conf 檔案新增 SSLProtocol 設定，透過黑 名單方式，關閉 SSL[5]。

	在 httpd.conf 加入以下設定： SSLProtocol all -SSLv2 -SSLv3 【IIS 修補方式】透過修改機碼的方式，關閉 SSL[6]。 a.開啟機碼設定(regedit.exe)，並至路徑[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL2.0] (SSL 3.0 路徑為[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL3.0]) b.在 SSL2.0 資料夾上按右鍵→新增→機碼，然後輸入「Server」 c.接著在剛剛建立 Server 的資料夾下按右鍵→新增→DWORD(32 位元)值，然後輸入「Enabled」 d.確認資料欄位值是否為「0x00000000 (0)」，若否，請手動將值改為 0。
參考資料	1.https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0800 (NVD) 2.https://www.owasp.org/index.php/Transport_Layer_Protection_Ch

	eat_Sheet (OWASP) 3.https://isaca.nl/dmdocuments/ISACA-NL-20140602.pdf (ISACA-OSSTMM) 4.https://access.redhat.com/solutions/1232233 5.http://httpd.apache.org/docs/2.0/ssl/ssl_howto.html 6.http://social.technet.microsoft.com/wiki/contents/articles/2249.how-to-disable-sslv2-on-a-windows-server-2008-and-windows-server-2008-r2-domain-controller-dsforum2wiki.aspx

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