張元成

寄件者: 國家資通安全會報技術服務中心 <ncert@icst.org.tw>
寄件日期: 2015年4月22日星期三 下午 3:39
收件者: ncert@icst.org.tw
主旨: [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-2015-0004)
簽名者: ncert@icst.org.tw

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-2015-0004	發布時間	Wed Apr 22 15:11:32 CST 2015
事件類型	漏洞預警	發現時間	Wed Apr 22 00:00:00 CST 2015
警訊名稱	HTTP.sys 中的資訊安全風險可能會允許遠端執行程式碼，弱點編號 CVE-2015-1635 (MS15-034)		
內容說明	微軟發布 HTTP.sys 可能會允許遠端執行程式碼之資訊安全更新，美國國家標準技術研究所(NIST)的國家弱點資料庫(NVD)發布弱點編號 CVE-2015-1635 [1-2]。 HTTP.sys 為處理 HTTP 要求的核心模式趨動程式，允許遠端使用者利用 Request Header 未檢查 Range 參數範圍漏洞，進行攻擊行為；成功利用這個資訊安全風險的攻擊者，能以系統帳戶權限層級執行任意程式碼或阻斷服務攻擊(DoS)。 請各機關檢視所屬 Windows 作業系統平台是否已針對微軟最新弱點進行修補。		
影響平台	1.Windows 7 2.Windows server 2008 R2 3.Windows 8 和 Windows 8.1 4.Windows Server 2012 和 Windows Server 2012 R2		
影響等級	高		
建議措施	1.請各機關檢視所屬受影響之 Windows 作業系統平台，是否已安裝資訊安全更新 KB3042553。各版本修補資訊與微軟資訊安全公告對應詳見[3]中?受影響的軟體?章節各版本修補連結，建議立即進行安全性更新。 2. MS15-034 漏洞檢測方式： 2.1 請至通報應變網站「資安文件下載區」下載檢測工具「MS15-035.exe」(須登入通報網站)。		

	2.2 請將檢測工具「MS15-035.exe」放置於受測主機執行 註：本工具僅提供本機使用，檢測通訊埠 80 2.3 檢測回應訊息說明： 【訊息回應 1】 test status: (未更新套件) The Host:127.0.0.1 is vulnerable 【訊息回應 2】 test status: (已上更新套件) The Host:127.0.0.1 has patched 【訊息回應 3】 test status: (無法判斷，可能伺服器非 windows) The Host:127.0.0.1 is unknown status
參考資料	1.美國國家弱點資料庫：https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1635 2.http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1635 3.微軟官方網站：https://technet.microsoft.com/zh-tw/library/security/ms15-034.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